Oracle FLEXCUBE
Security Management System User Manual
Release 5.0.0.0.0
Part No E52077-01

ORACLE

Table of Contents (index)

1. SMS 3
1.1. 7011 - Event Log Inquiry 4
1.2. 752 - Reset Primary Password 7
1.3. 753 - Enable/Disable User 10
1.4. 755 - Modify Login Status 13
1.5. 756 - User Prohibited Passwords 15
1.6. 757 - Inquiry For Logged In Users 18
1.7. 758 - Inquiry For Password 20
1.8. 766 - Secondary Password Expiry Date 23
1.9. 767 - Reset Secondary Password 26
1.10. 768 - Change Primary Password 29
1.11. 769 - Change Secondary Password 32
1.12. AT002 - Audit Trail Financial Transactions Inquiry 35
1.13. BA777 - Audit Trail Inquiry for Non-Financial Txns* 40
1.14. BAM04 - BA Audit Tasks Maintenance-Inquire 48
1.15. BAM10 - Restricted Accounts Maintenance 51
1.16. SM11A - Inquiry On Logged In Users 54
1.17. SMM02 - User Profile Maintenance 56
1.18. SMM03 - Task Profile Maintenance 66
1.19. SMM09 - User Prohibited Password Maintenance 70
1.20. SMM12 - User Class Cross Reference Maintenance 73
1.21. SMM13 - Template Transaction Limits 76

1. SMS

The FLEXCUBE Retail Security Management System (SMS) provides a security envelope within which, all the FLEXCUBE Retail application modules are executed. SMS maintains and controls access to users in the FLEXCUBE Retail system and ensures that only authorized users are allowed to use the system. Security definitions are broadly categorized into two parts namely host security definition and branch security definition. For the purpose of security and centralized control, it is recommended that all the security related definitions users are created at the HO and branch security definitions are important attributes of the user are modified at HO and downloaded to the branches. All the users of the bank can be broadly classified depending upon their role and seniority. Such classification is represented in FLEXCUBE Retail using templates. All the FLEXCUBE Retail transactions are linked to one or more such templates to define the access to the transactions for the respective class of users. Each user needs to have a user profile defined in the system. This user profile is linked to one of the templates.

1.1. 7011 - Event Log Inquiry

User logged in from different computer under a core banking network is allowed (although concurrent user log-ins is not allowed).

Using this option you can log the IP's under which the user ID was entered in the posting date. The system displays the date, time and action performed. The system displays the date, time and action performed.

Definition Prerequisites

Not Applicable

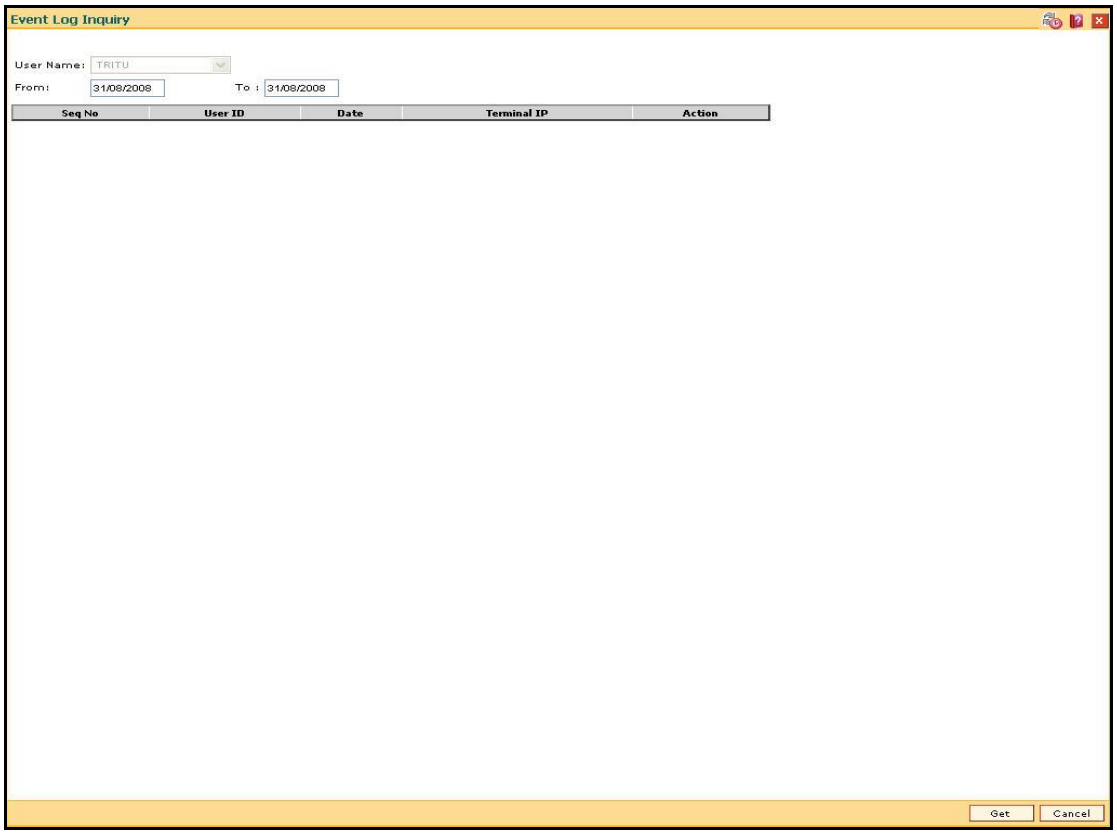
Modes Available

Not Applicable

To perform event log inquiry

1. Type the fast path **7011** and click **Go** or navigate through the menus to **Transaction Processing > Internal Transactions > Inquiries > Event Log Inquiry**.
2. The system displays the **Event Log Inquiry** screen.

Event Log Inquiry



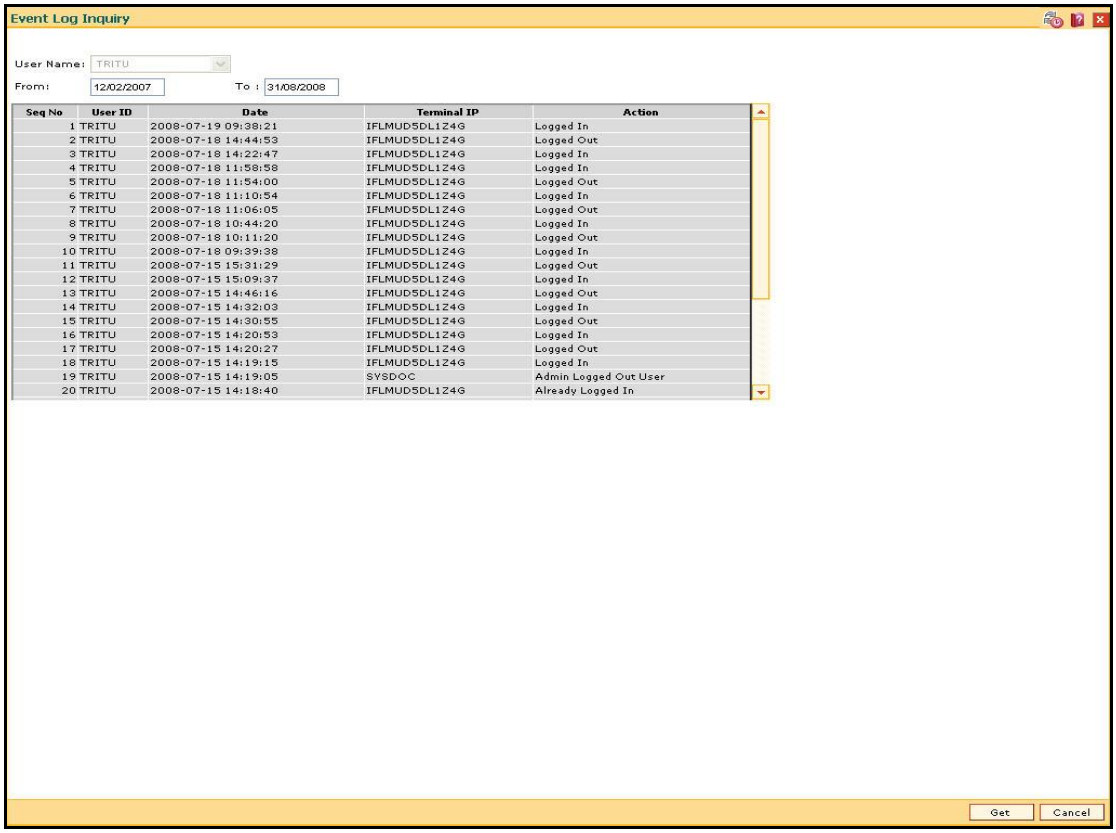
Field Description

Field Name	Description
User Name	[Display] This field displays the name of the user who is logged in.
From	[Mandatory, dd/mm/yyyy] Type the date from which the event log inquiry is to be made.
To	[Mandatory, dd/mm/yyyy] Type the date till which the event log inquiry is to be made.

Column Name	Description
Seq No	[Display] This column displays the sequence number of the event.
User ID	[Display] This column displays the user id.
Date	[Display] This column displays the date and time of the event.
Terminal IP	[Display] This column displays the terminal IP from where the user had logged in.
Action	[Display] This column displays the action performed by the user.

3. Enter the from and to date.
4. Click the **Get** button. The system displays the event log details.

Event Log Inquiry


Event Log Inquiry
User Name: TRITU
From: 12/02/2007
To : 31/08/2008
Seq No | User ID | Date | Terminal IP | Action
1 TRITU 2008-07-19 09:38:21 IFLMUD5DL1Z4G Logged In
2 TRITU 2008-07-18 14:44:53 IFLMUD5DL1Z4G Logged Out
3 TRITU 2008-07-18 14:22:47 IFLMUD5DL1Z4G Logged In
4 TRITU 2008-07-18 11:58:58 IFLMUD5DL1Z4G Logged In
5 TRITU 2008-07-18 11:54:00 IFLMUD5DL1Z4G Logged Out
6 TRITU 2008-07-18 11:10:54 IFLMUD5DL1Z4G Logged In
7 TRITU 2008-07-18 11:06:05 IFLMUD5DL1Z4G Logged Out
8 TRITU 2008-07-18 10:44:20 IFLMUD5DL1Z4G Logged In
9 TRITU 2008-07-18 10:11:20 IFLMUD5DL1Z4G Logged Out
10 TRITU 2008-07-18 09:39:38 IFLMUD5DL1Z4G Logged In
11 TRITU 2008-07-15 15:31:29 IFLMUD5DL1Z4G Logged Out
12 TRITU 2008-07-15 15:09:37 IFLMUD5DL1Z4G Logged In
13 TRITU 2008-07-15 14:46:16 IFLMUD5DL1Z4G Logged Out
14 TRITU 2008-07-15 14:32:03 IFLMUD5DL1Z4G Logged In
15 TRITU 2008-07-15 14:30:55 IFLMUD5DL1Z4G Logged Out
16 TRITU 2008-07-15 14:20:53 IFLMUD5DL1Z4G Logged In
17 TRITU 2008-07-15 14:20:27 IFLMUD5DL1Z4G Logged Out
18 TRITU 2008-07-15 14:19:15 IFLMUD5DL1Z4G Logged In
19 TRITU 2008-07-15 14:19:05 SYSDOC Admin Logged Out User
20 TRITU 2008-07-15 14:18:40 IFLMUD5DL1Z4G Already Logged In
Get
Cancel

5. Click the **Cancel** button.

1.2. 752 - Reset Primary Password

Using this option you can reset the password without entering the old one .This option is used by the system administrator to reset the password if the user has forgotten his password or if the SM does not want the user to log into the system. If the user knows the new password, he will be prompted to change it on login.

Definition Prerequisites

- SMM02 - User Profile Maintenance

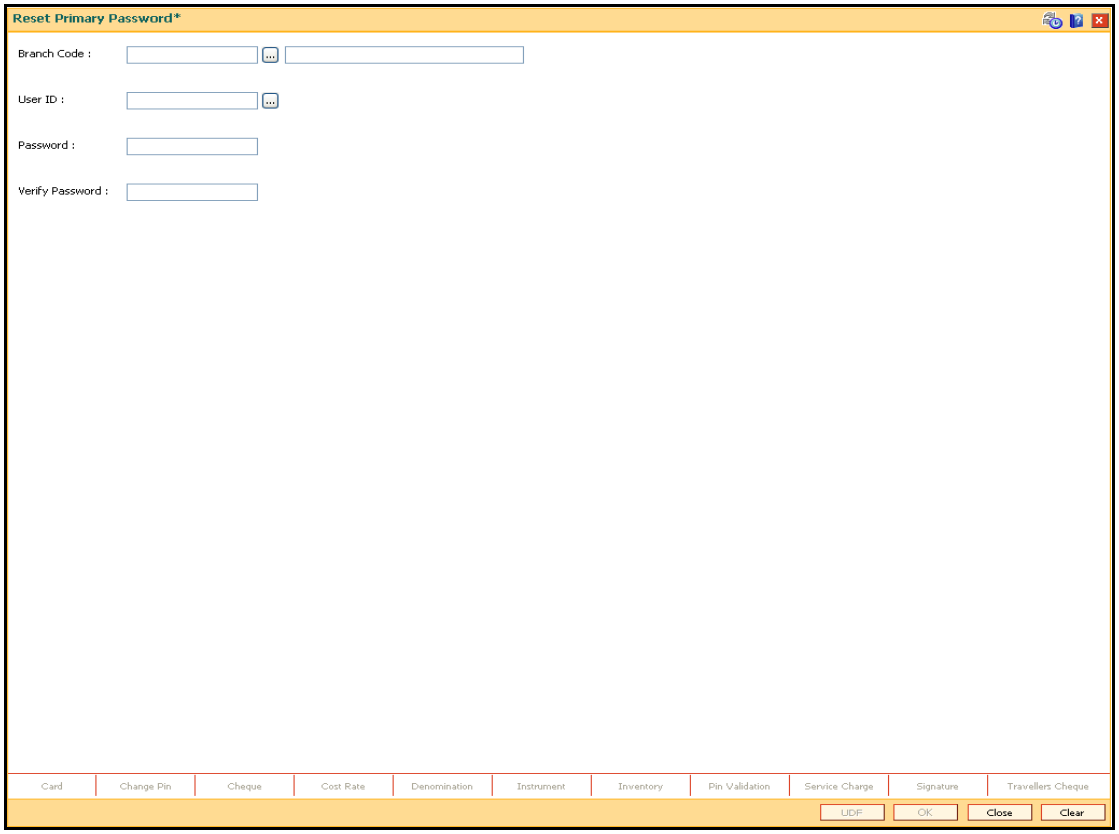
Modes Available

Not Applicable

To reset the primary password

1. Type the fast path **752** and click **Go** or navigate through the menus to **Transaction Processing > Internal Transactions > Security > Reset primary password**.
2. The system displays the **Reset Primary Password** screen.

Reset Primary Password

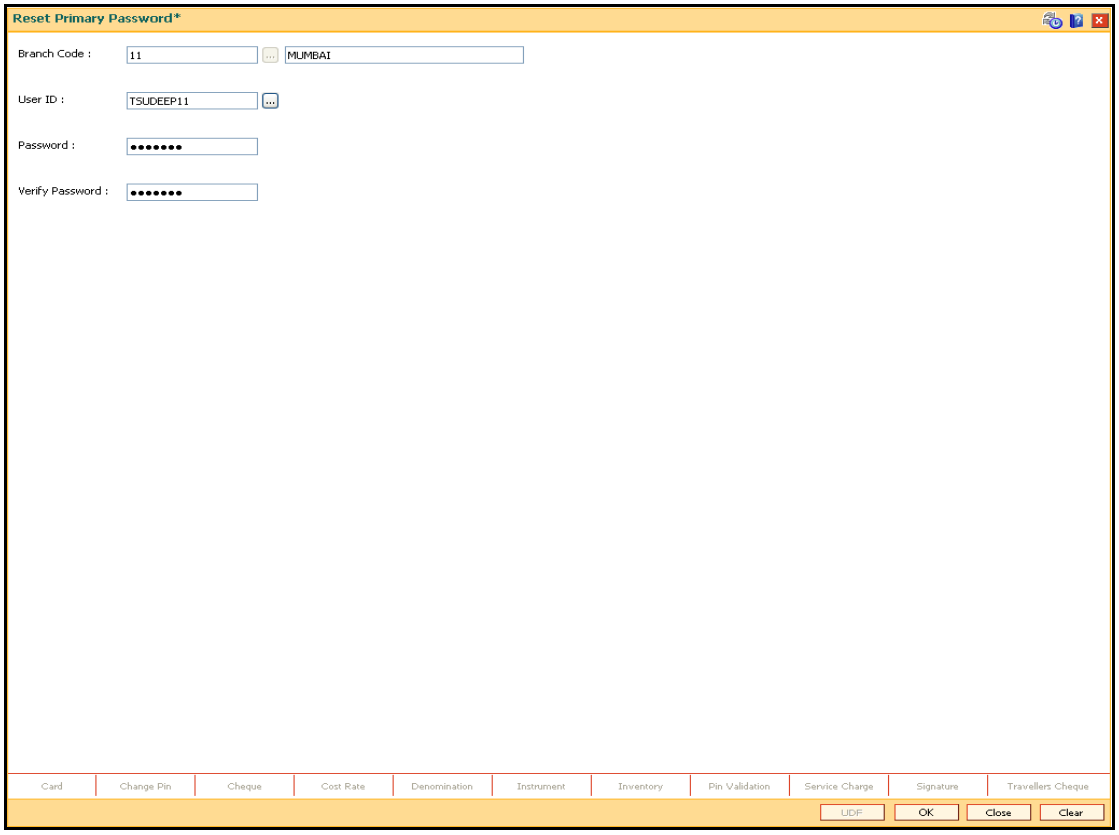


Field Description

Field Name	Description
Branch Code	[Mandatory, Numeric, Four, Pick List] Type the branch code or select it from the pick list. The name of the branch is displayed in the adjacent field.
User ID	[Mandatory, Pick List] Select the user ID whose password you want to reset from the pick list. These user IDs are added and maintained in the **User Profile Maintenance** (Fast Path: SMM02) option.
Password	[Mandatory, Alphanumeric, 10] Type the password, for the selected user ID. The password should have a minimum of six characters. It should be a combination of an uppercase and lowercase letter and a numeric digit. The password cannot have three or more successive characters or digits. For example, abc, xyz etc.
Verify Password	[Mandatory, Alphanumeric, 10] Type the new password to verify it. It should be the same as entered in the **Password** field.

3. Select the user ID from the drop-down list.
4. Enter the required information in the various fields.

Reset Primary Password



5. Click the **Ok** button.

1.3. 753 - Enable/Disable User

Using this option you can enable/ disable a user of any branch through single administrator log in. The user IDs are created in the **User Profile Maintenance** (Fast Path: SMM02) option.

Note: The system cannot disable the already logged in users.

Definition Prerequisites

- SMM02 - User Profile Maintenance

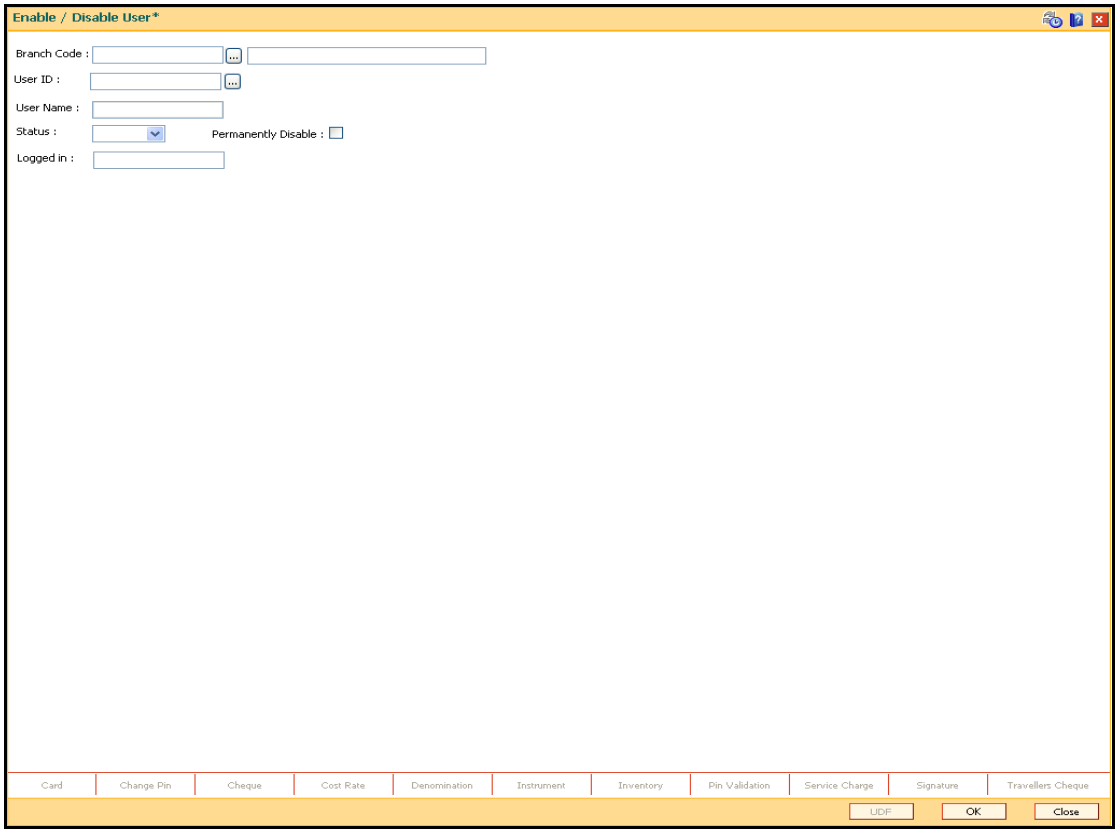
Modes Available

Not Applicable

To enable or disable a user

1. Type the fast path **753** and click **Go** or navigate through the menus to **Transaction Processing > Internal Transactions > Security > Enable / Disable user**.
2. The system displays the **Enable / Disable User** screen.

Enable / Disable User

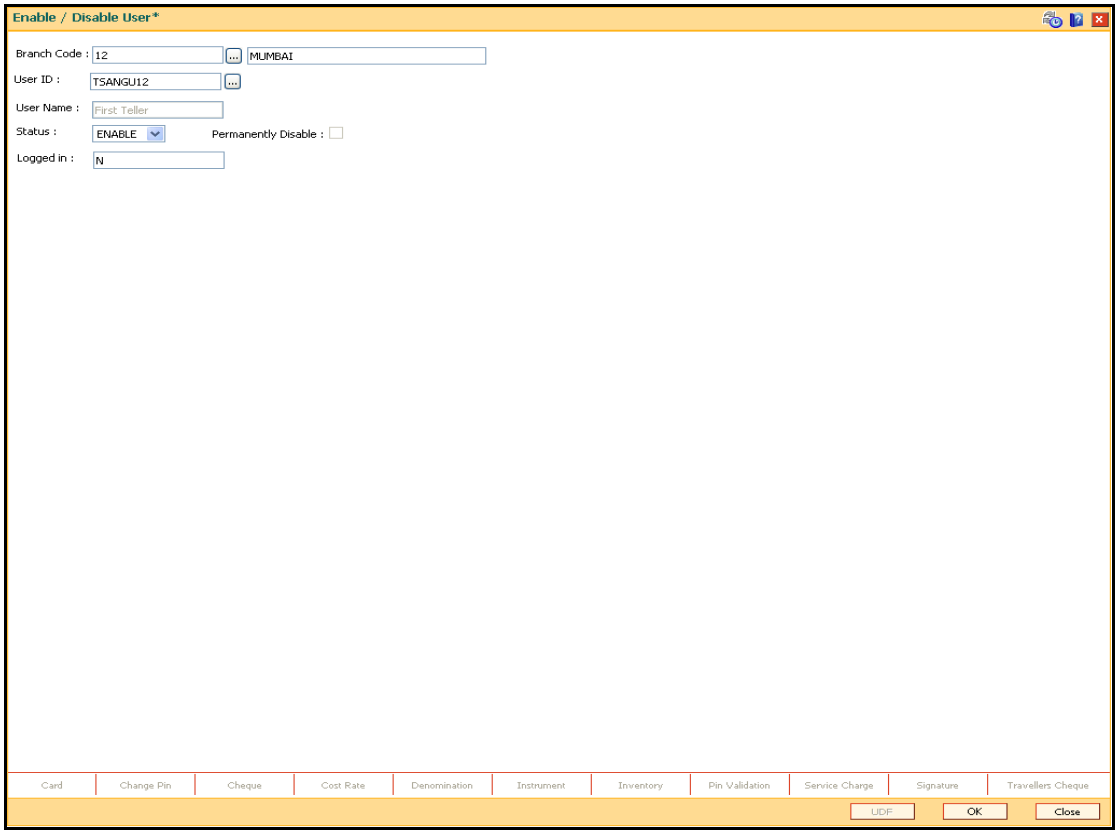


Field Description

Field Name	Description
Branch Code	[Mandatory, Numeric, Four, Pick List] Type the branch code or select it from the pick list. The name of the branch is displayed in the adjacent field.
User Id	[Mandatory, Pick List] Select the ID of the user, who has to be enabled or disabled, from the pick list. These user ID's are maintained in the **User Profile Maintenance** (Fast Path: SMM02) option.
User Name	[Display] This field displays the name of the user for the selected user ID.
Status	[Mandatory, Drop-Down] Select the status from the drop-down list. The options are: • ENABLE • DISABLE • LOCK : Select this option to unlock a user ID.
Permanently Disable	[Conditional, Check Box] Select the check box to permanently disable a user. This field is enabled only if **DISABLE** option is selected in the **Status** drop-down list.
Logged in	[Display] This field displays the logged in status of the user. The options are: • Y: User is logged in. • N: User is not logged in.

3. Select the branch code and user ID from the pick list.

Enable / Disable User



4. If the user is disabled, the system displays the message "User is Disabled. Do You Want to Enable".
5. If the user is not logged in, the system displays the "User Not Logged in. Want to Disable?".
6. Click the **Ok** button.

1.4. 755 - Modify Login Status

Using this option you are forcibly logged out of the system. This option is used when you have logged into **FLEXCUBE** and the application/system crashes. When you try to login after the system is restored, it does not allow, as the system still maintains the user status as logged in. Also, the system will not permit a login more than once. In such cases this option is used to modify the login status.

Definition Prerequisites

- SMM02 - User Profile Maintenance

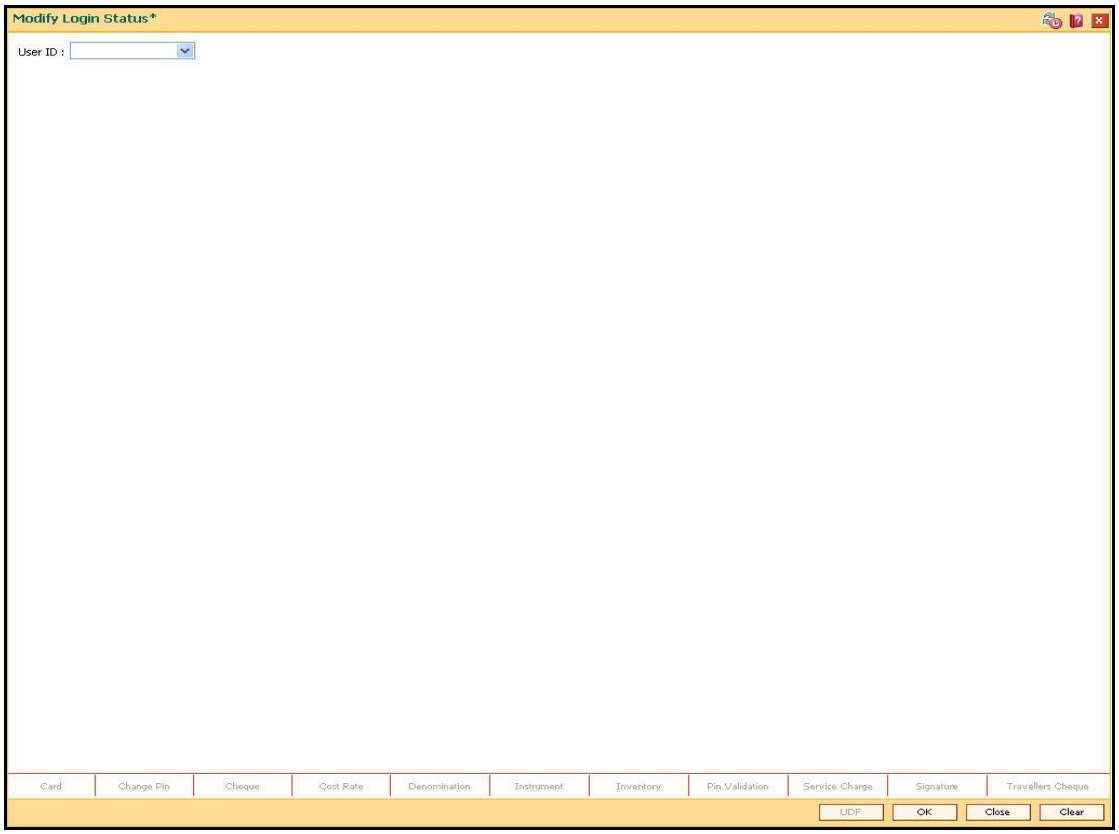
Modes Available

Not Applicable

To modify login status

1. Type the fast path **755** and click **Go** or navigate through the menus to **Transaction Processing > Internal Transactions > Security > Modify Login Status**.
2. The system displays the **Modify Login Status** screen.

Modify Login Status

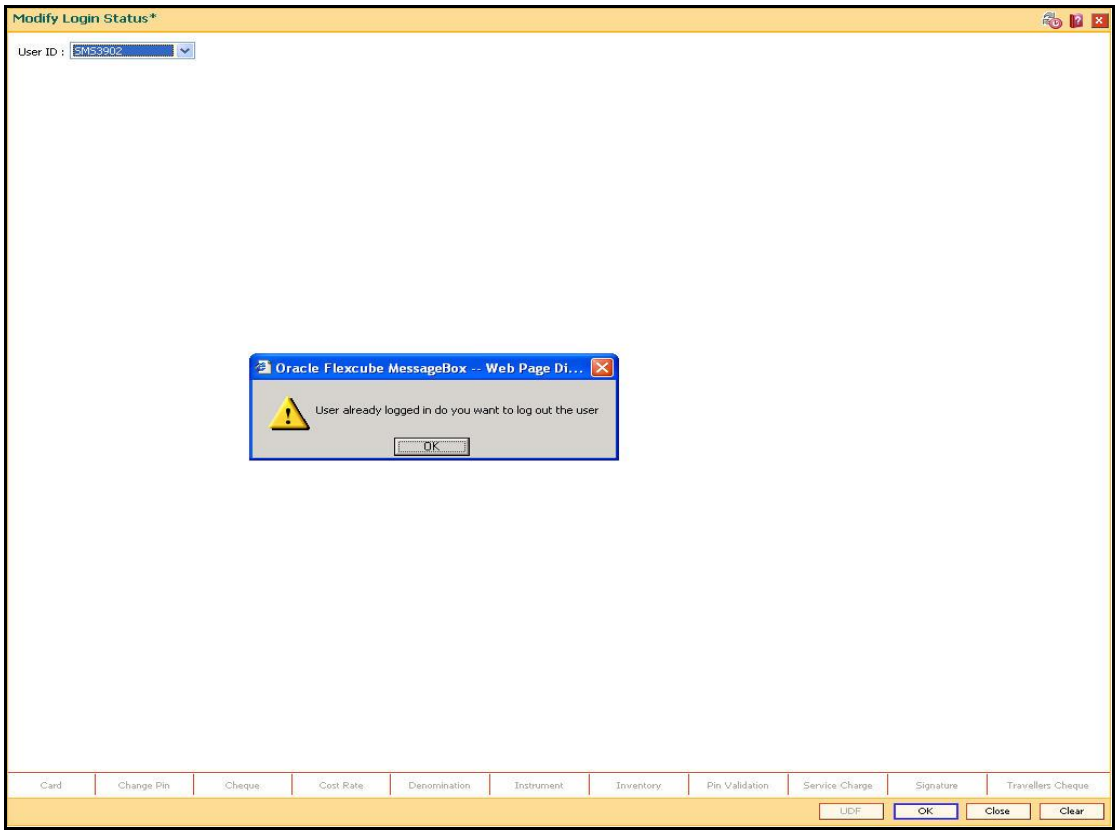


Field Description

Field Name	Description
User ID	[Mandatory, Drop-Down] Select the user ID of the user, whose login status is to be modified, from the drop-down list. These user ID's are maintained in the **Defining User Profile** (Fast Path: SMM02) option.

3. Select the user ID from the drop-down list.

Modify Login Status



4. The system displays the message "User already logged in do you want to log out the user". Click the **Ok** button.
5. Click the **OK** button.

1.5. 756 - User Prohibited Passwords

Using this option you can define those passwords which should not be used by particular user in the bank. These restrictions on using the password shall apply to only that user in the bank. These are commonly used words specific to the person such as place of residence, spouse name, name of son/daughters, etc.

Definition Prerequisites

- SMM02 - User Profile Maintenance

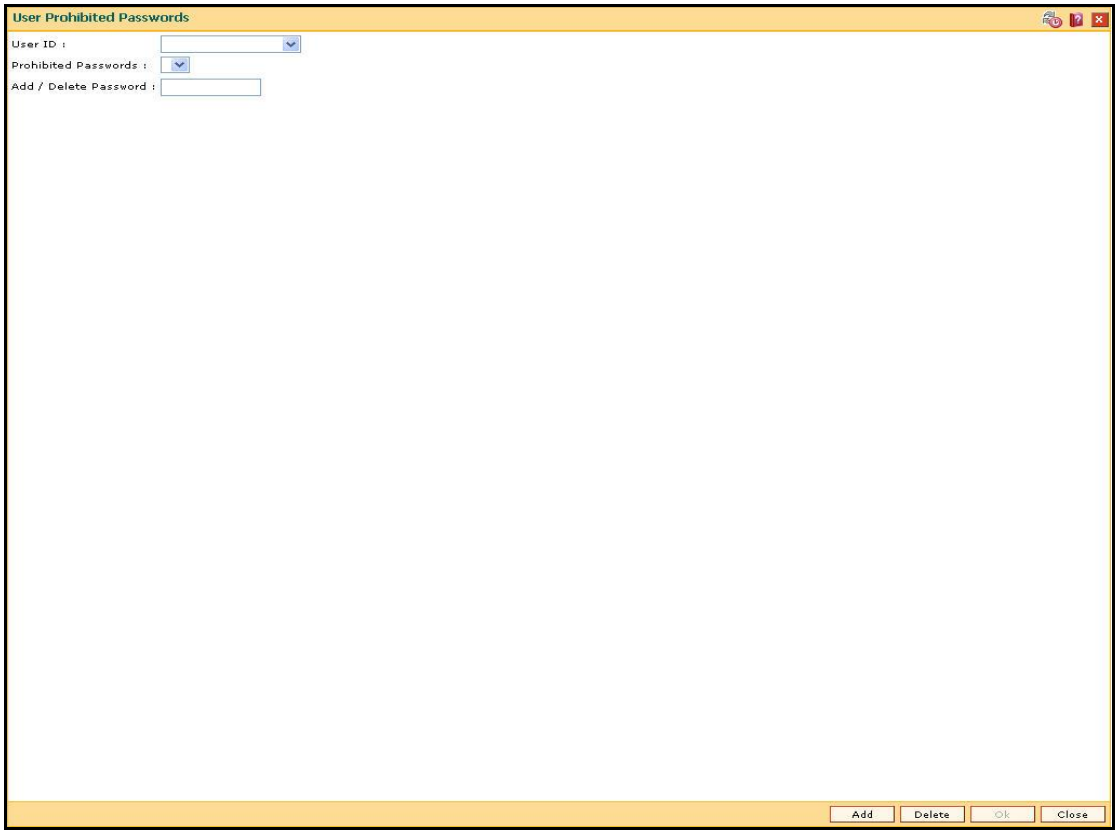
Modes Available

Not Applicable

To change the defined prohibited password

1. Type the fast path **756** and click **Go** or navigate through the menus to **Transaction Processing > Internal Transactions > Security > User Prohibited Passwords**.
2. The system displays the **User Prohibited Passwords** screen.

User Prohibited Passwords

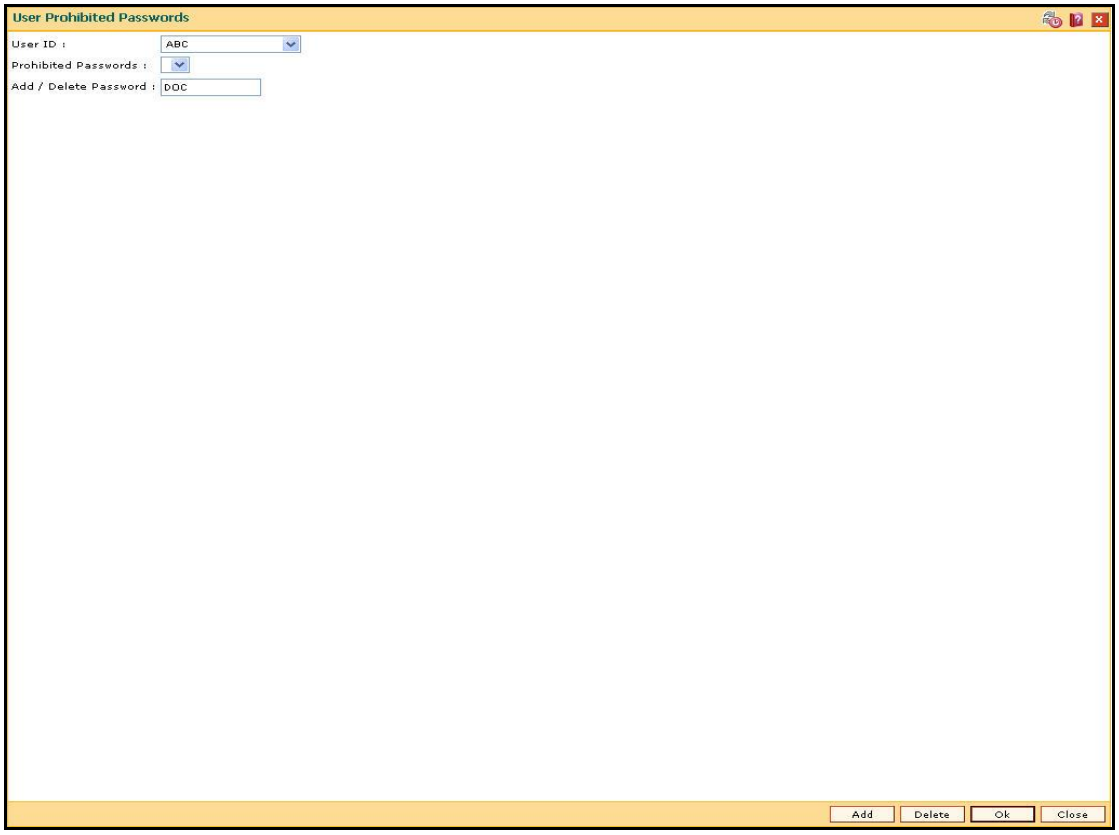


Field Description

Field Name	Description
User ID	[Mandatory, Drop-Down] Select the user ID from the drop-down list. These user IDs are added and maintained in the **Defining User Profile** (Fast Path: SMM02) option.
Prohibited Passwords	[Mandatory, Drop-Down] Select the prohibited password from the drop-down list. These prohibited passwords are added and maintained centrally in the User **Prohibited Password** option.
Add / Delete Password	[Mandatory, Alphanumeric, Eight] Type the password that is to be added or deleted. It should be a combination of an uppercase and lowercase letter and a numeric digit. The password cannot have three or more successive characters or digits. For example, abc, xyz etc.

3. Click the **Add** button.
4. The system displays the message "You are in Add option". Click the **OK** button.
5. The system displays the message "Data will be refreshed..Proceed?". Click the **OK** button.
6. The system refreshes the **User Prohibited Passwords** screen.
7. Select the user ID from the drop-down list.
8. Enter the prohibited password.

User Prohibited Passwords



9. Click the **Ok** button.
10. The system adds the prohibited password for that user ID.

1.6. 757 - Inquiry For Logged In Users

Using this option you can view the list of users that are logged in to the system in their own branch.

The system provides information on user ID, user name, the terminal ID in which the user has logged in and the login date and time. You can refresh the screen to get the latest status.

Definition Prerequisites

Not Applicable

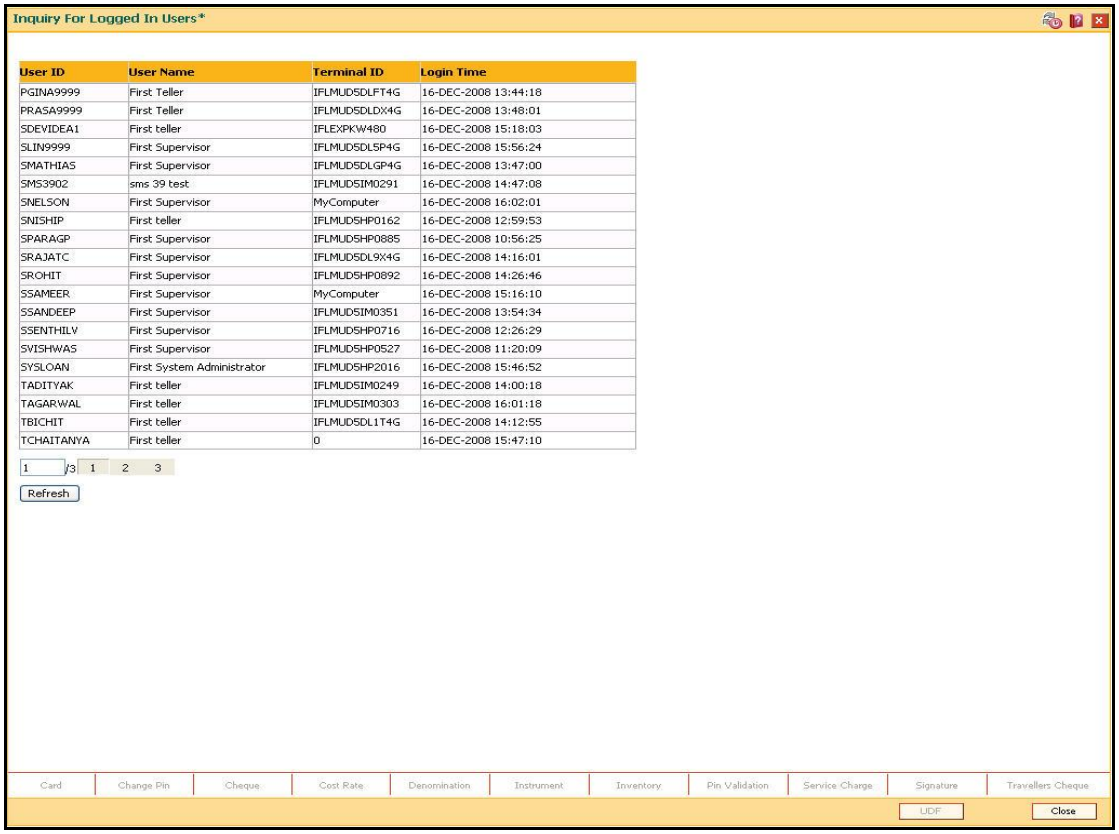
Modes Available

Not Applicable

To view a list of currently logged in users

1. Type the fast path **757** and click **Go** or navigate through the menus to **Transaction Processing > Internal Transactions > Security > Inquiry For Logged In Users**.
2. The system displays the **Inquiry For Logged In Users** screen.

Inquiry For Logged In Users


Inquiry For Logged In Users*
User ID
User Name
Terminal ID
Login Time
PGINA9999 First Teller IFLMUD5DLFT4G 16-DEC-2008 13:44:18
PRASA9999 First Teller IFLMUD5DLDX4G 16-DEC-2008 13:48:01
SDEVIDEA1 First teller IFLEXPKW480 16-DEC-2008 15:18:03
SLIN9999 First Supervisor IFLMUD5DL5P4G 16-DEC-2008 15:56:24
SMATHIAS First Supervisor IFLMUD5DLGP4G 16-DEC-2008 13:47:00
SMS3902 sms 39 test IFLMUD5IM0291 16-DEC-2008 14:47:08
SNELSON First Supervisor MyComputer 16-DEC-2008 16:02:01
SNISHIP First teller IFLMUD5HP0162 16-DEC-2008 12:59:53
SPARAGP First Supervisor IFLMUD5HP0885 16-DEC-2008 10:56:25
SRAJATC First Supervisor IFLMUD5DL9X4G 16-DEC-2008 14:16:01
SROHIT First Supervisor IFLMUD5HP0892 16-DEC-2008 14:26:46
SSAMEER First Supervisor MyComputer 16-DEC-2008 15:16:10
SSANDEEP First Supervisor IFLMUD5IM0351 16-DEC-2008 13:54:34
SSENTHILV First Supervisor IFLMUD5HP0716 16-DEC-2008 12:26:29
SVISHWAS First Supervisor IFLMUD5HP0527 16-DEC-2008 11:20:09
SYSLOAN First System Administrator IFLMUD5HP2016 16-DEC-2008 15:46:52
TADITYAK First teller IFLMUD5IM0249 16-DEC-2008 14:00:18
TAGARWAL First teller IFLMUD5IM0303 16-DEC-2008 16:01:18
TBICHIT First teller IFLMUD5DL1T4G 16-DEC-2008 14:12:55
TCHAITANYA First teller 0 16-DEC-2008 15:47:10
1 /3 1 2 3
Refresh
Card
Change Pin
Cheque
Cost Rate
Denomination
Instrument
Inventory
Pin Validation
Service Charge
Signature
Travellers Cheque
UDF
Close

Field Description

Column Name	Description
User ID	[Display] This column displays the user ID for all those users who are currently logged into the system.
User Name	[Display] This column displays the list of users who are currently logged into the system.
Terminal ID	[Display] This column displays the identification code of the terminal where each user has logged into the system.
Login Time	[Display] This column displays the login date and time when the users have logged into the system.

3. The system displays the users who are currently logged in to the system.
4. Click the **Refresh** button to refresh the screen with the latest details.

1.7. 758 - Inquiry For Password

Using this option you can view the password details of the registered users . The system provides information on dual password facility available for the user IDs, primary password change due date, secondary password change due date, whether the system manger can reset the password, etc.

The inquiry about the passwords of the users will be useful for the supervisor mainly to keep track of the users for whom password reset is to be done, and if password change by Supervisor is allowed for the user.

You can change the primary/secondary passwords by using **Change Primary Password** (Fast Path: 768) and **Change Secondary Password** (Fast Path: 769) options.

Definition Prerequisites

Not Applicable

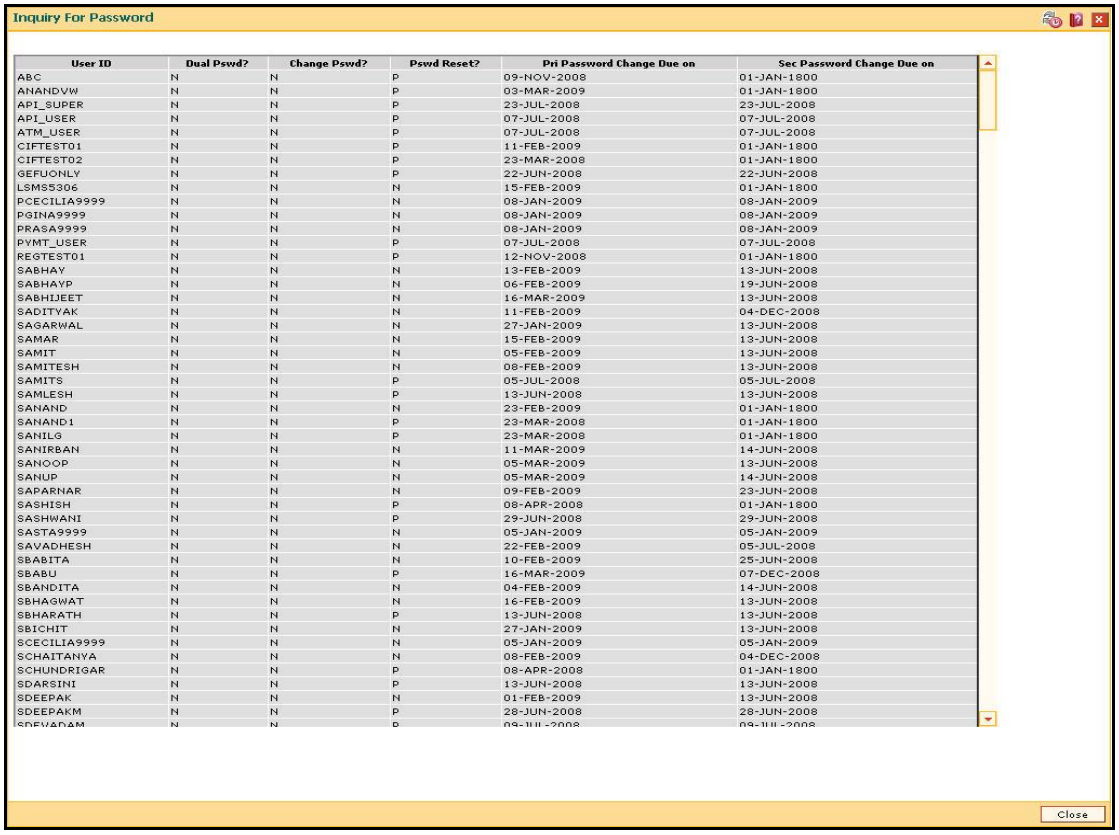
Modes Available

Not Applicable

To view password details

1. Type the fast path **758** and click **Go** or navigate through the menus to **Transaction Processing > Internal Transactions > Security > Inquiry For Password**.
2. The system displays the **Inquiry For Password** screen.

Inquiry For Password



User ID	Dual Pswd?	Change Pswd?	Pswd Reset?	Pri Password Change Due on	Sec Password Change Due on
ABC	N	N	P	09-NOV-2008	01-JAN-1800
ANANDVW	N	N	P	03-MAR-2009	01-JAN-1800
API_SUPER	N	N	P	23-JUL-2008	23-JUL-2008
API_USER	N	N	P	07-JUL-2008	07-JUL-2008
ATM_USER	N	N	P	07-JUL-2008	07-JUL-2008
CIFTEST01	N	N	P	11-FEB-2009	01-JAN-1800
CIFTEST02	N	N	P	23-MAR-2008	01-JAN-1800
GEFUONLY	N	N	P	22-JUN-2008	22-JUN-2008
LSMS5306	N	N	N	15-FEB-2009	01-JAN-1800
PCECILIA9999	N	N	N	08-JAN-2009	08-JAN-2009
PGINA9999	N	N	N	08-JAN-2009	08-JAN-2009
PRASA9999	N	N	N	08-JAN-2009	08-JAN-2009
PYMT_USER	N	N	P	07-JUL-2008	07-JUL-2008
REGTEST01	N	N	P	12-NOV-2008	01-JAN-1800
SABHAY	N	N	N	13-FEB-2009	13-JUN-2008
SABHAYP	N	N	N	06-FEB-2009	19-JUN-2008
SABHIJEET	N	N	N	16-MAR-2009	13-JUN-2008
SADITYAK	N	N	N	11-FEB-2009	04-DEC-2008
SAGARWAL	N	N	N	27-JAN-2009	13-JUN-2008
SAMAR	N	N	N	15-FEB-2009	13-JUN-2008
SAMIT	N	N	N	05-FEB-2009	13-JUN-2008
SAMITESH	N	N	N	08-FEB-2009	13-JUN-2008
SAMITS	N	N	P	05-JUL-2008	05-JUL-2008
SAMLESH	N	N	P	13-JUN-2008	13-JUN-2008
SANAND	N	N	N	23-FEB-2009	01-JAN-1800
SANAND1	N	N	P	23-MAR-2008	01-JAN-1800
SANILG	N	N	P	23-MAR-2008	01-JAN-1800
SANIRBAN	N	N	N	11-MAR-2009	14-JUN-2008
SANOOP	N	N	N	05-MAR-2009	13-JUN-2008
SANUP	N	N	N	05-MAR-2009	14-JUN-2008
SAPARNAR	N	N	N	09-FEB-2009	23-JUN-2008
SASHISH	N	N	P	08-APR-2008	01-JAN-1800
SASHWANI	N	N	P	29-JUN-2008	29-JUN-2008
SASTA9999	N	N	N	05-JAN-2009	05-JAN-2009
SAVADHESH	N	N	N	22-FEB-2009	05-JUL-2008
SBABITA	N	N	N	10-FEB-2009	25-JUN-2008
SBABU	N	N	P	16-MAR-2009	07-DEC-2008
SBANDITA	N	N	N	04-FEB-2009	14-JUN-2008
SBHAGWAT	N	N	N	16-FEB-2009	13-JUN-2008
SBHARATH	N	N	P	13-JUN-2008	13-JUN-2008
SBICHIT	N	N	N	27-JAN-2009	13-JUN-2008
SCECILIA9999	N	N	N	05-JAN-2009	05-JAN-2009
SCHAITANYA	N	N	N	08-FEB-2009	04-DEC-2008
SCHUNDRIGAR	N	N	P	08-APR-2008	01-JAN-1800
SDARSINI	N	N	P	13-JUN-2008	13-JUN-2008
SDEEPAK	N	N	N	01-FEB-2009	13-JUN-2008
SDEEPAKM	N	N	P	28-JUN-2008	28-JUN-2008
SDEVADAM	N	N	P	09-JUL-2008	09-JUL-2008

Field Description

Column Name	Description
User ID	[Display] This column displays the list of user IDs of the system.
Dual Pswd?	[Display] This column displays whether the user ID has dual password facility or not. The system displays: • Y: if the user ID has dual password facility. • N: if the user ID does not have dual password facility.
Change Pswd?	[Display] This column displays whether the user can change his/her password or not. The system displays: • Y: if the user can change the password. • N: if the user cannot change the password.

Column Name	Description
Pswd Reset?	[Display] This column displays the status of the user's password. The system displays: • P: if the security manager resets the user's password • N: if the user logs in and changes the password
Pri Password Change Due on	[Display] This column displays the date on which the primary password is due for change.
Sec Password Change Due on	[Display] This column displays the date on which the secondary password is due for change.

3. Click the **Close** button.

1.8. 766 - Secondary Password Expiry Date

Using this option you can change the date on which a particular user's secondary password will expire.

While the users can view the password details like primary password change due date, secondary password change due date, etc. in **Inquiry For Password** (Fast Path: 758) option they can change the primary/secondary passwords by using **Change Primary Password** (Fast Path: 768) and **Change Secondary Password** (Fast Path: 769) options.

Definition Prerequisites

- SMM02 - User Profile Maintenance

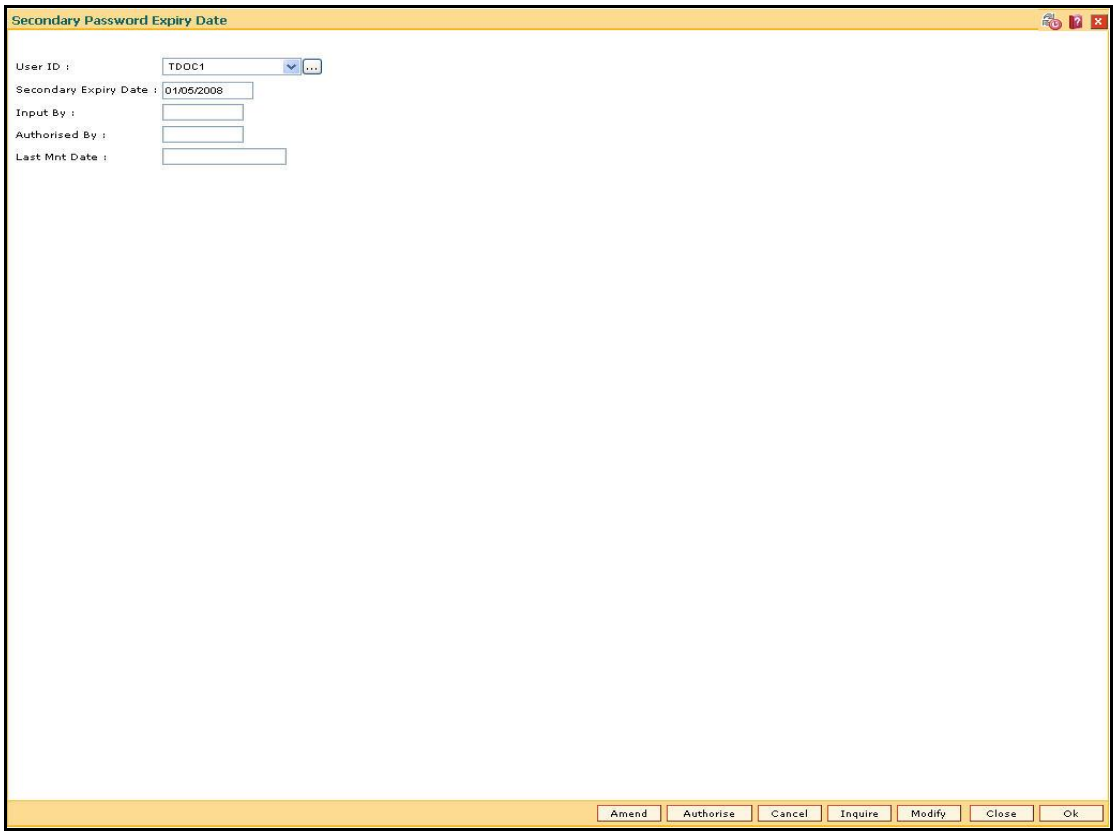
Modes Available

Not Applicable

To modify the secondary password expiry date

1. Type the fast path **766** and click **Go** or navigate through the menus to **Transaction Processing > Internal Transactions > Security > Secondary Password Expiry Date**.
2. The system displays the **Secondary Password Expiry Date** screen.

Secondary Password Expiry Date

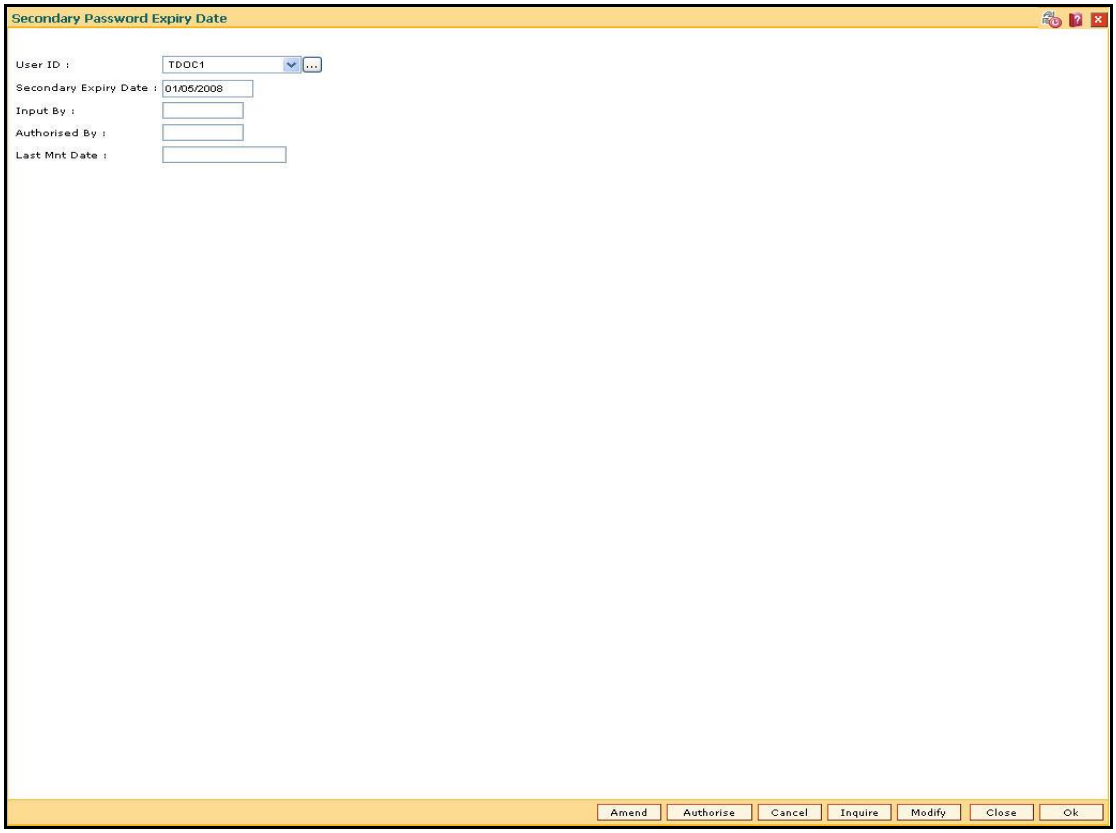


Field Description

Field Name	Description
User ID	[Mandatory, Pick List] Select the user ID from the pick list. These user IDs are added and maintained in the **Defining User Profile** (Fast Path: SMM02) option.
Secondary Expiry Date	[Mandatory, Numeric, dd/mm/yyyy] Type the new secondary expiry date for the password, which is greater than the current posting date. By default, this field displays the old expiry date. This date specifies the validity period of the password.
Input By	[Display] This field displays the user who has created the record. In the **Inquiry** mode, this field displays the user who had last maintained the record.
Authorised By	[Display] This field displays the user who has authorised the record.
Last Mnt. Date	[Display] This field displays the date and time when the record was last maintained.

3. Click the **Modify** button.
4. The system displays the message "Data will be refreshed..Proceed?". Click the **OK** button.
5. The system refreshes the **Secondary Password Expiry Date** screen.
6. Select the user id from the drop-down list or select it from the pick list.
7. Modify the relevant information in the various fields.

Secondary Password Expiry Date



8. Click the **Ok** button.
9. The system displays the message "The transaction completed successfully... Authorizsation Pending". Click the **Ok** button.
10. The modified secondary password expiry date is reflected once the transaction is authorised.

1.9. 767 - Reset Secondary Password

Using this option you can reset the password without entering the old one . This option is used by the system administrator to forcibly to reset the password if the user has forgotten his password or if the SM does not want the user to log into the system. If the user knows the new password, he will be prompted to change it on login.

Definition Prerequisites

- SMM02 - User Profile Maintenance

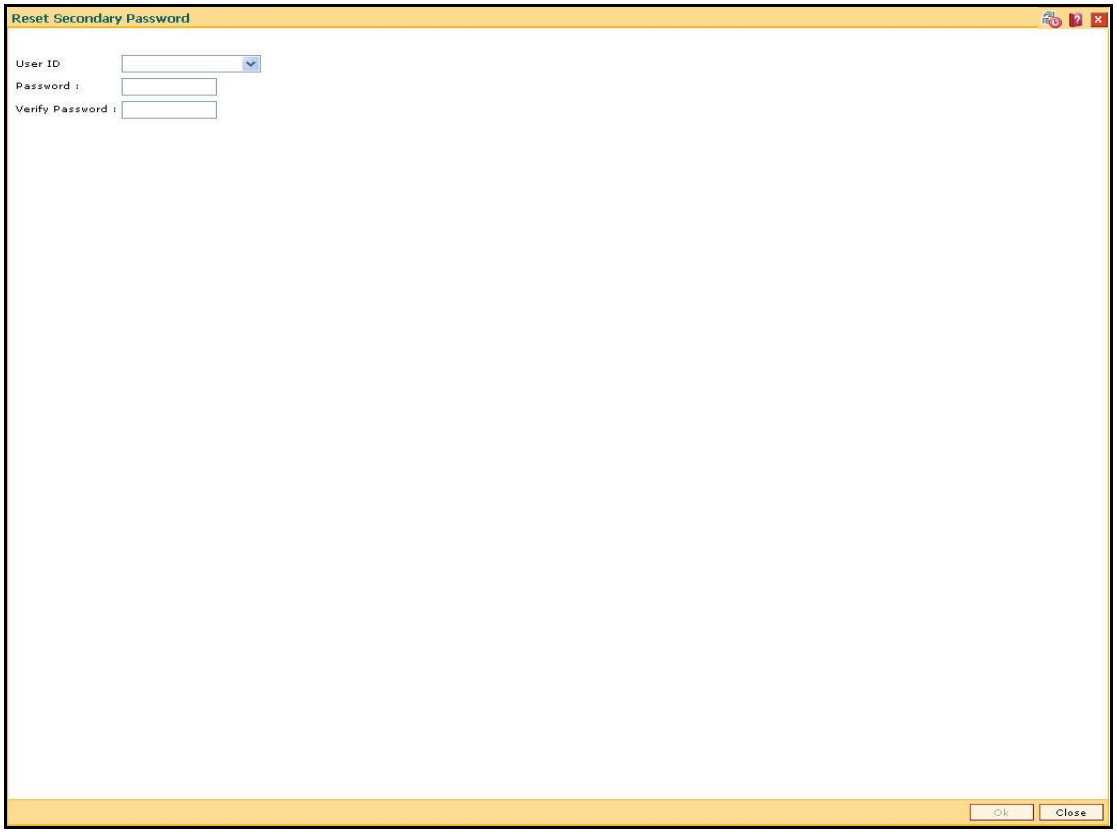
Modes Available

Not Applicable

To reset the secondary password

1. Type the fast path **767** and click **Go** or navigate through the menus to **Transaction Processing > Internal Transactions > Security > Reset Secondary Password**.
2. The system displays the **Reset Secondary Password** screen.

Reset Secondary Password

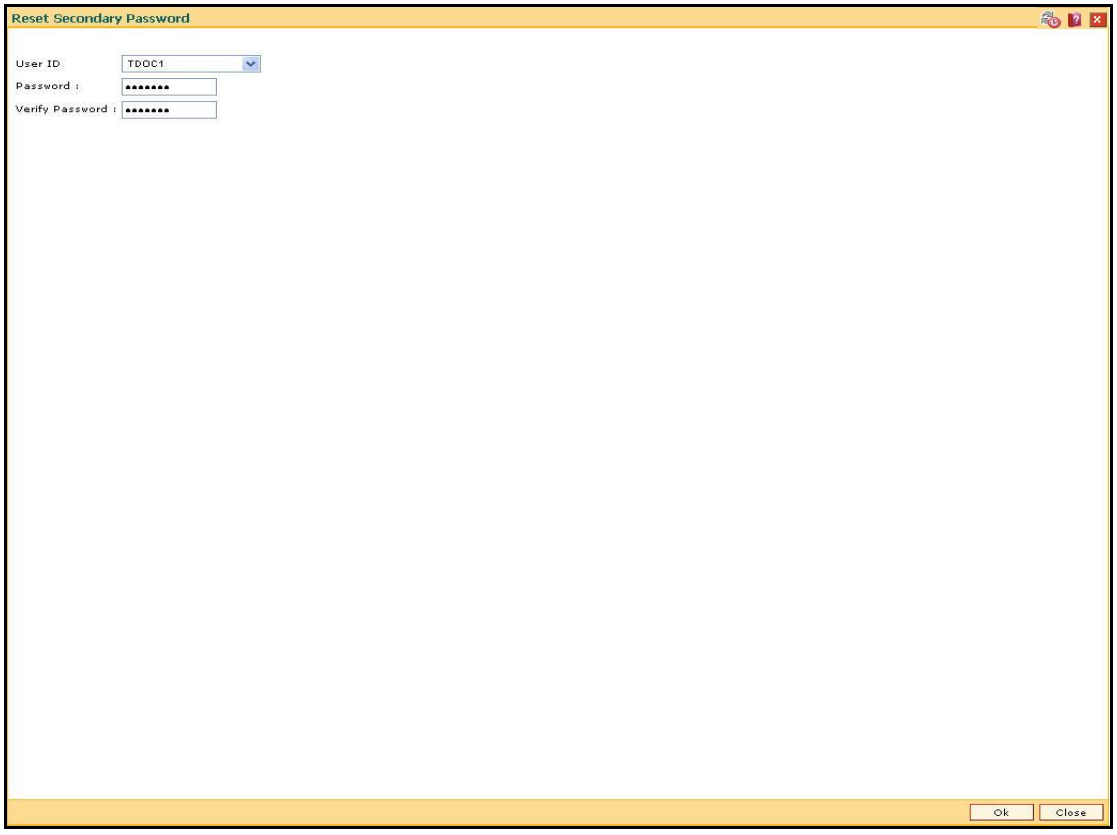


Field Description

Field Name	Description
User ID	[Mandatory, Drop-Down] Select the user ID from the drop-down list. These user IDs are added and maintained in the **Defining User Profile** (Fast Path: SMM02) option.
Password	[Mandatory, Alphanumeric, 14] Type the new secondary password. It should have a minimum of eight characters. It should be a combination of an uppercase and lowercase letter and a numeric digit. The password cannot have three or more successive characters or digits. For example, abc, xyz etc.
Verify Password	[Mandatory, Alphanumeric, 14] Type the new password to verify it. It should be the same as entered in the **Password** field.

3. Select the user ID from the drop-down list.
4. Enter the required information in the various fields.

Reset Secondary Password



5. Click the **Ok** button.

1.10. 768 - Change Primary Password

Using is option you can change your own password using the **Change Primary Password** option. You cannot use the passwords which are prohibited specifically in **User Prohibited Passwords** (Fast Path: 756) option. These are commonly used words specific to the person such as place of residence, spouse name, name of son/daughter, etc.

Definition Prerequisites

Not Applicable

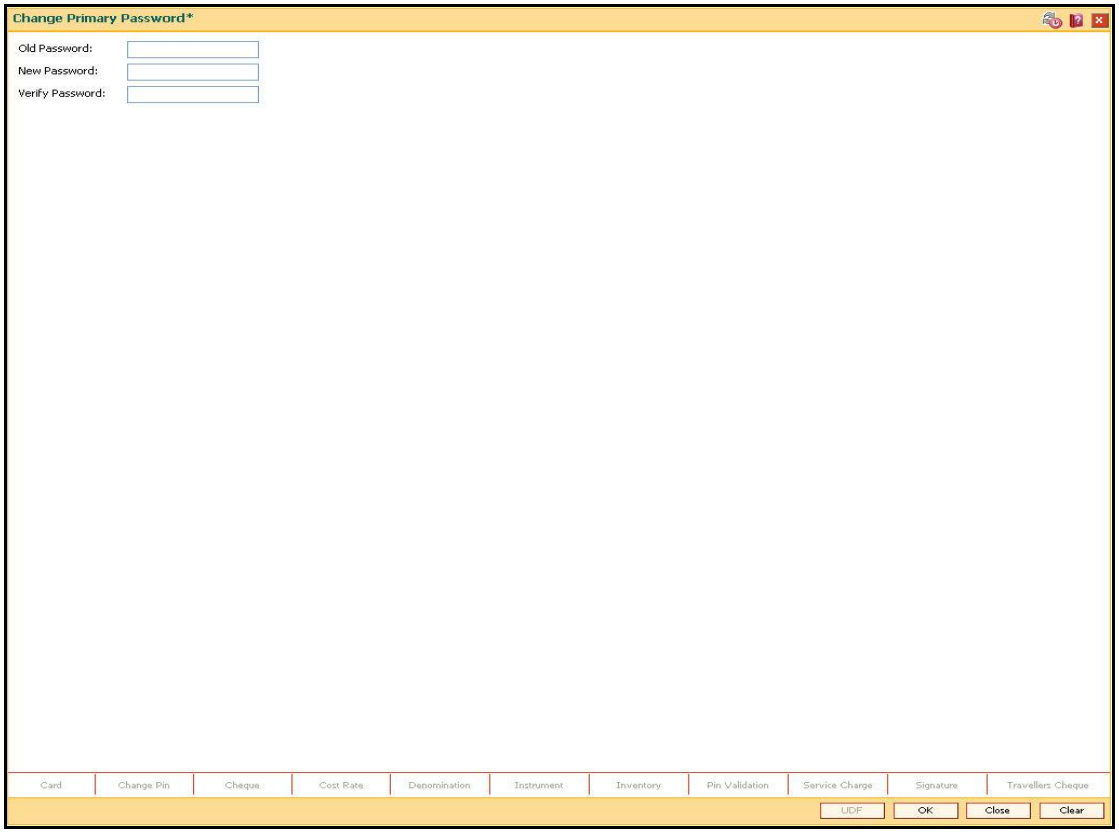
Modes Available

Not Applicable

To change primary password

1. Type the fast path **768** and click **Go** or navigate through the menus to **Transaction Processing > Internal Transactions > Security > Change Primary Password** .
2. The system displays the **Change Primary Password** screen.

Change Primary Password

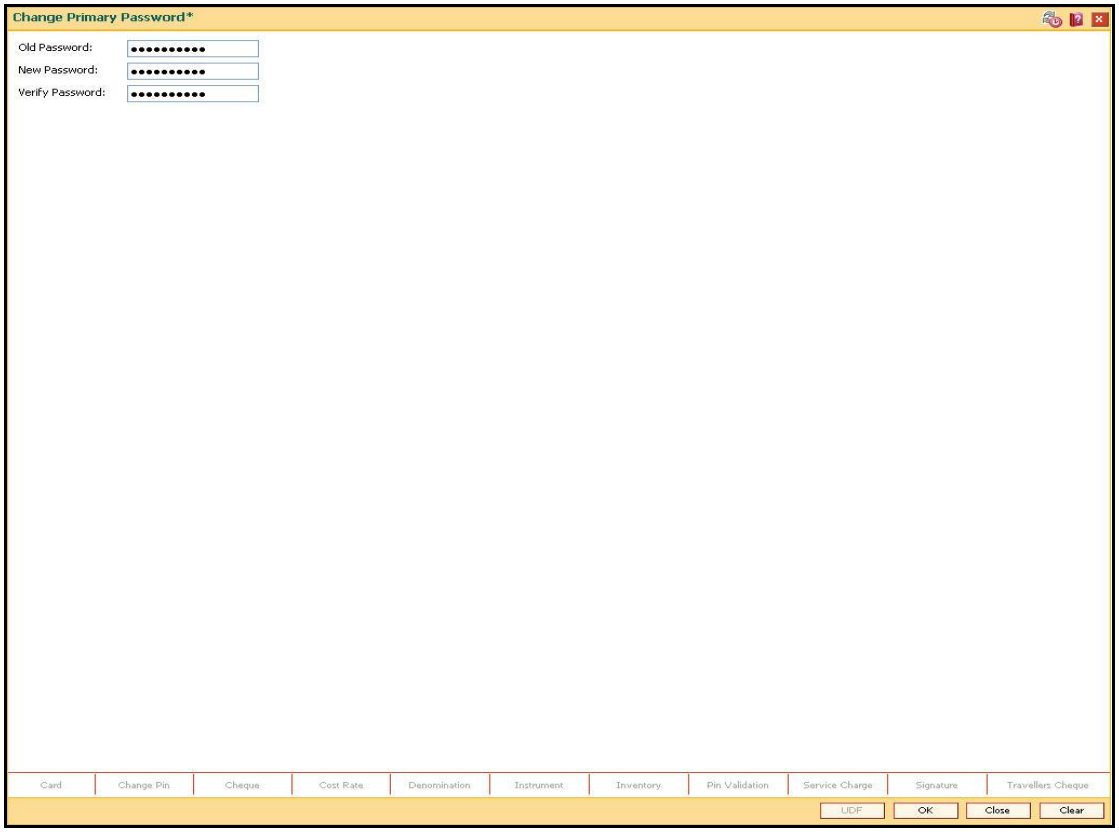


Field Description

Field Name	Description
Old Password	[Mandatory, Alphanumeric, 10] Type the valid current or old password.
New Password	[Mandatory, Alphanumeric, 10] Type the new password, which you would like to use. The password should have a minimum of six characters. It should be a combination of an uppercase and lowercase letter, and a numeric digit. The password cannot have three or more successive characters or digits. For example, abc, xyz etc.
Verify Password	[Mandatory, Alphanumeric, 10] Type the new password again to verify it.

3. Type the old password.
4. Type the new password and re-type it for confirmation.

Change Primary Password



5. Click the **Ok** button.
6. The system changes the primary password.

1.11. 769 - Change Secondary Password

Using this option you can change your own secondary password using the **Change Secondary Password** option. You cannot use the passwords which are prohibited specifically in **User Prohibited Passwords** (Fast Path: 756) option. These are commonly used words specific to the person such as place of residence, spouse name, name of son/daughter, etc.

Definition Prerequisites

Not Applicable

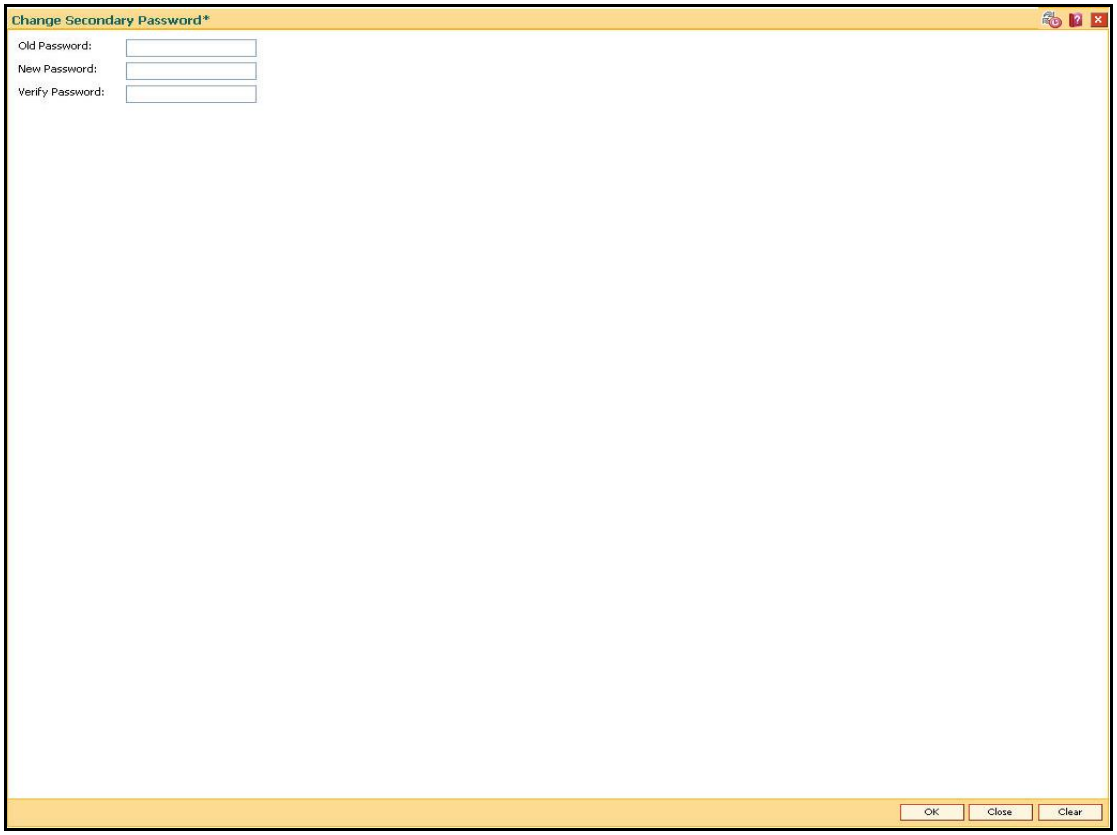
Modes Available

Not Applicable

To change secondary password

1. Type the fast path **769** and click **Go** or navigate through the menus to **Transaction Processing > Internal Transactions > Security > Change Secondary Password**.
2. The system displays the **Change Secondary Password** screen.

Change Secondary Password

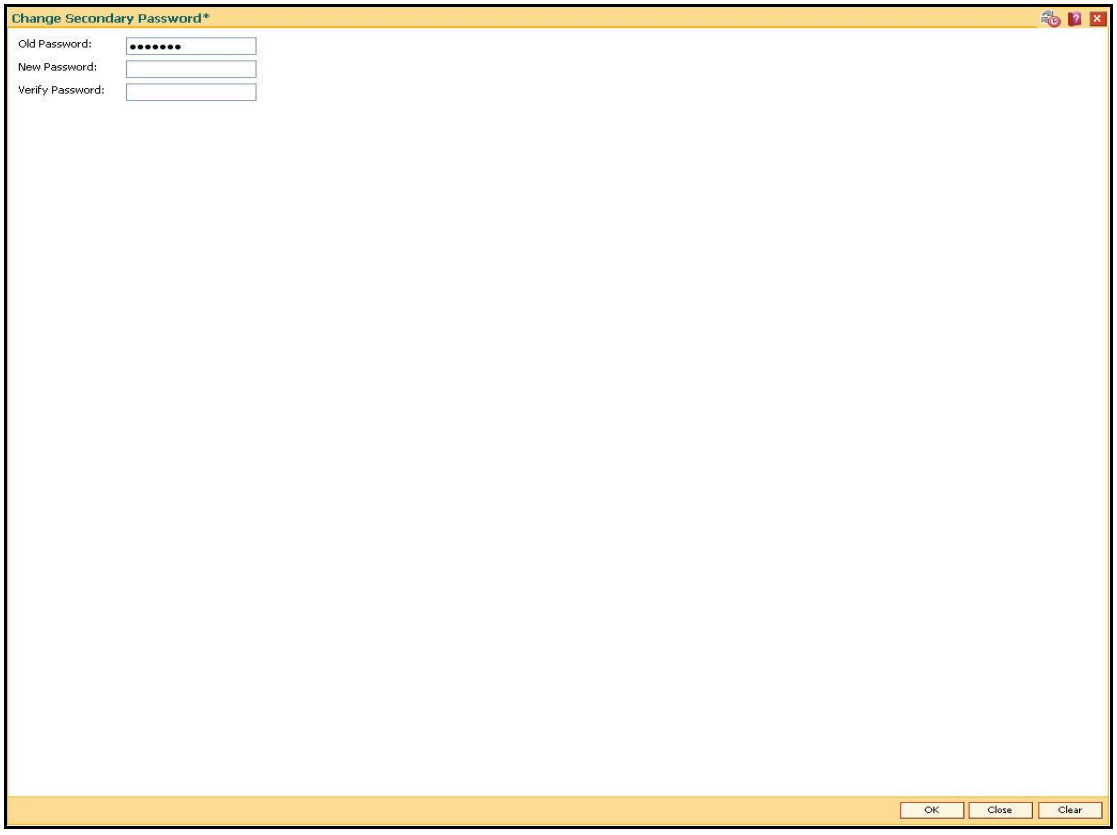


Field Description

Field Name	Description
Old Password	[Mandatory, Alphanumeric, 14] Type the valid current or old password.
New Password	[Mandatory, Alphanumeric, 14] Type the new password you would like to use. The password should have a minimum of eight characters. It should be a combination of an uppercase and lowercase letter, and a numeric digit. The password cannot have three or more successive characters or digits. For example, abc, xyz etc.
Verify Password	[Mandatory, Alphanumeric, 14] Type the new password to verify it.

3. Type the old password.
4. Type the new password and re-type it for confirmation.

Change Secondary Password



5. Click the **Ok** button.
6. The system changes the secondary password.

1.12. AT002 - Audit Trail Financial Transactions Inquiry

Using this option you can view the audit trail of financial transactions performed on **Oracle FLEXCUBE**. The audit trail can be queried using this maintenance on any of the following parameters:

- Originating Branch
- Date Range
- Teller ID or Super ID
- Customer ID or Account Number
- Transaction mnemonic and/or Amount range
- Type of transaction, Transaction number

Definition Prerequisites

- Financial Transactions should have been performed

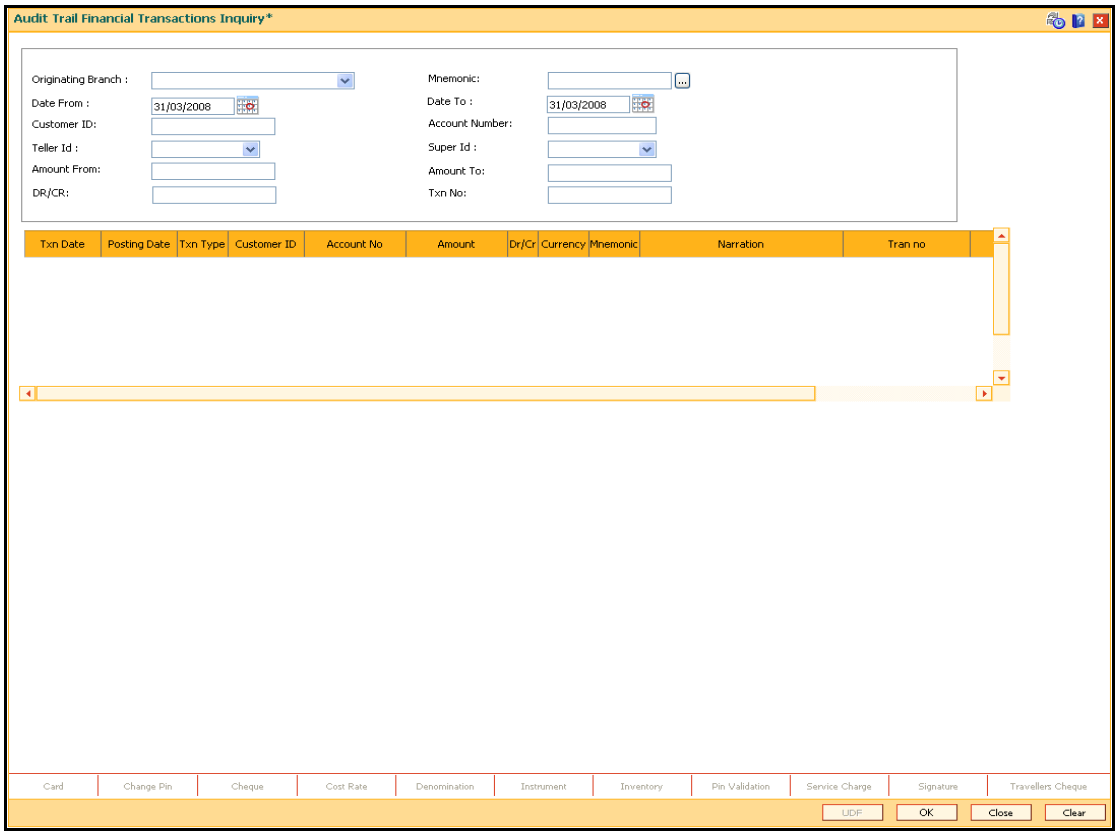
Modes Available

Not Applicable

To inquire on audit trail

1. Type the fast path **AT002** and click **Go** or navigate through the menus to **Transaction Processing > Internal Transactions > Inquiries > Audit Trail Financial Transactions Inquiry.**
2. The system displays the **Audit Trail Financial Transactions Inquiry** screen.

Audit Trail Financial Transactions Inquiry



Field Description

Field Name	Description
Originating Branch	[Mandatory, Drop-Down] Select the originating branch, for which the audit trail is required, from the drop-down list.
Mnemonic	[Optional, Pick List] Select the maintenance task code to be be audited from the pick list.
Date From	[Mandatory, Pick List, dd/mm/yyyy] Select the date from which the data has to be retrieved from the pick list.
Date To	[Mandatory, Pick list, dd/mm/yyyy] Select the date up to which the data has to be retrieved from the pick list.
Customer ID	[Optional, Alphanumeric, 10] Type the id of the customer on whom the maintenance was done.

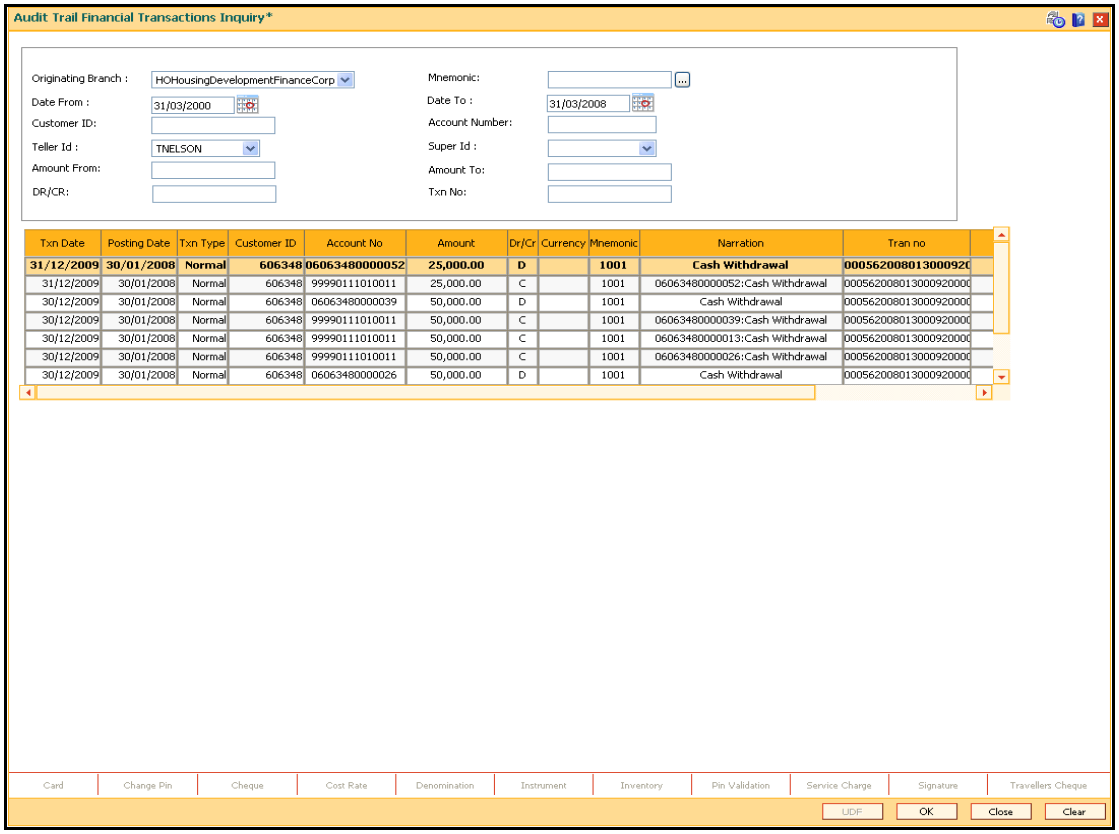
Field Name	Description
Account Number	[Optional, Numeric, 16] Type the account number on which the maintenance was done.
Teller ID	[Mandatory, Drop-Down] Select the id of the teller who has performed the maintenance from the drop-down list.
Super ID	[Optional, Drop-Down] Select the id of the authoriser who has authorised the maintenance from the drop-down list.
Amount From	[Optional, Alphanumeric, 13, Two] Type the minimum amount from which the records are to be displayed.
Amount To	[Optional, Alphanumeric, 13, Two] Type the maximum amount upto which the records are to be displayed.
DR/CR	[Optional, Character, One] Enter the type of transaction. You can type D or C to view the debit or credit transactions.
Txn No	[Optional, Alphanumeric, 40] Type the transaction number for which the records are to be displayed.

Column Name	Description
Txn Date	[Display] This column displays the date of transaction.
Posting Date	[Display] This column displays the posting date.
Txn Type	[Display] This column displays the type of transaction.
Customer ID	[Display] This column displays the id of the customer on whom the maintenance was done.
Account No	[Display] This column displays the account number on whom the maintenance was done.

Column Name	Description
Amount	[Display] This column displays the transaction amount.
Dr/Cr	[Display] This column displays the type of transaction i.e Debit or Credit.
Currency	[Display] This column displays the account currency.
Mnemonic	[Display] This column displays the transaction mnemonic.
Narration	[Display] This column displays the narration for the transaction.
Tran No	[Display] This column displays the transaction number.
Teller ID	[Display] This column displays the id of the teller who has performed the transaction.
Auth ID	[Display] This column displays the id of the authoriser who has authorised the transaction.

3. Select the originating branch and teller id from the drop-down list.
4. Enter the date range for which transactions are to be displayed.
5. Click the **Ok** button. The system displays the financial tansactions based on the criteria entered.

Audit Trail Financial Transactions Inquiry


Audit Trail Financial Transactions Inquiry*
Originating Branch : HOHousingDevelopmentFinanceCorp
Date From : 31/03/2000
Customer ID:
Teller Id : TNELSON
Amount From:
DR/CR:
Mnemonic:
Date To : 31/03/2008
Account Number:
Super Id :
Amount To:
Txn No:
Txn Date | Posting Date | Txn Type | Customer ID | Account No | Amount | Dr/Cr | Currency | Mnemonic | Narration | Tran no
31/12/2009 | 30/01/2008 | Normal | 606348 | 06063480000052 | 25,000.00 | D | | 1001 | Cash Withdrawal | 00056200801300092
31/12/2009 | 30/01/2008 | Normal | 606348 | 99990111010011 | 25,000.00 | C | | 1001 | 06063480000052:Cash Withdrawal | 00056200801300092
30/12/2009 | 30/01/2008 | Normal | 606348 | 06063480000039 | 50,000.00 | D | | 1001 | Cash Withdrawal | 00056200801300092
30/12/2009 | 30/01/2008 | Normal | 606348 | 99990111010011 | 50,000.00 | C | | 1001 | 06063480000039:Cash Withdrawal | 00056200801300092
30/12/2009 | 30/01/2008 | Normal | 606348 | 99990111010011 | 50,000.00 | C | | 1001 | 06063480000013:Cash Withdrawal | 00056200801300092
30/12/2009 | 30/01/2008 | Normal | 606348 | 99990111010011 | 50,000.00 | C | | 1001 | 06063480000026:Cash Withdrawal | 00056200801300092
30/12/2009 | 30/01/2008 | Normal | 606348 | 06063480000026 | 50,000.00 | D | | 1001 | Cash Withdrawal | 00056200801300092
Card | Change Pin | Cheque | Cost Rate | Denomination | Instrument | Inventory | Pin Validation | Service Charge | Signature | Travellers Cheque
UDF | OK | Close | Clear

6. Click the **Close** button.

1.13. BA777 - Audit Trail Inquiry for Non-Financial Txns*

A bank can view the trail of both financial and non-financial transactions performed on **FLEXCUBE**. Only those non-financial transactions for which audit trails are required can be inquired in this inquiry. This requirement is maintained in Audit Task Maintenance. The audit trail can be queried using this maintenance on any of the following parameters:

- Originating Branch
- Task ID
- Date Range
- Teller ID
- Authorizer ID
- Action

Definition Prerequisites

- BAM04 - BA Audit Tasks Maintenance-Inquire

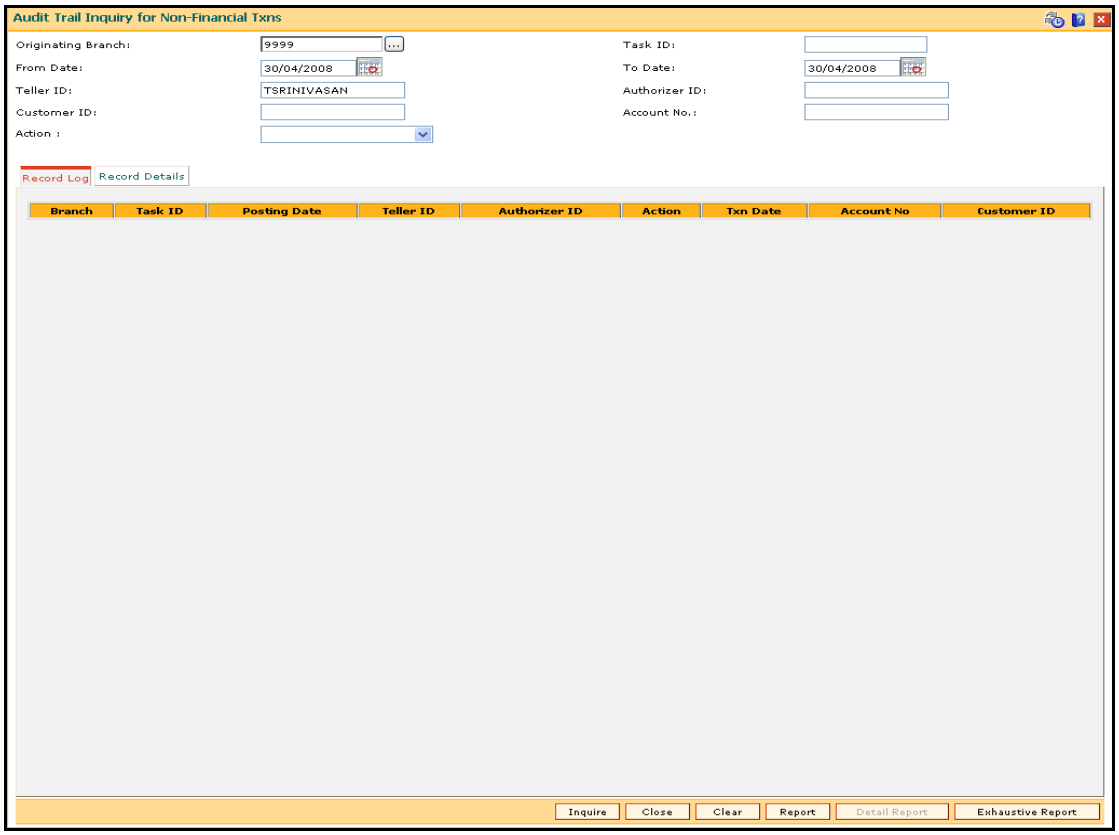
Modes Available

Not Applicable

To inquire on audit trail

1. Type the fast path **BA777** and click **Go** or navigate through the menus to **Global Definitions > Other >Audit Trail Inquiry for Non-Financial Txns**.
2. The system displays the **Audit Trail Inquiry for Non-Financial Txns** screen.

Audit Trail Inquiry for Non-Financial Txns



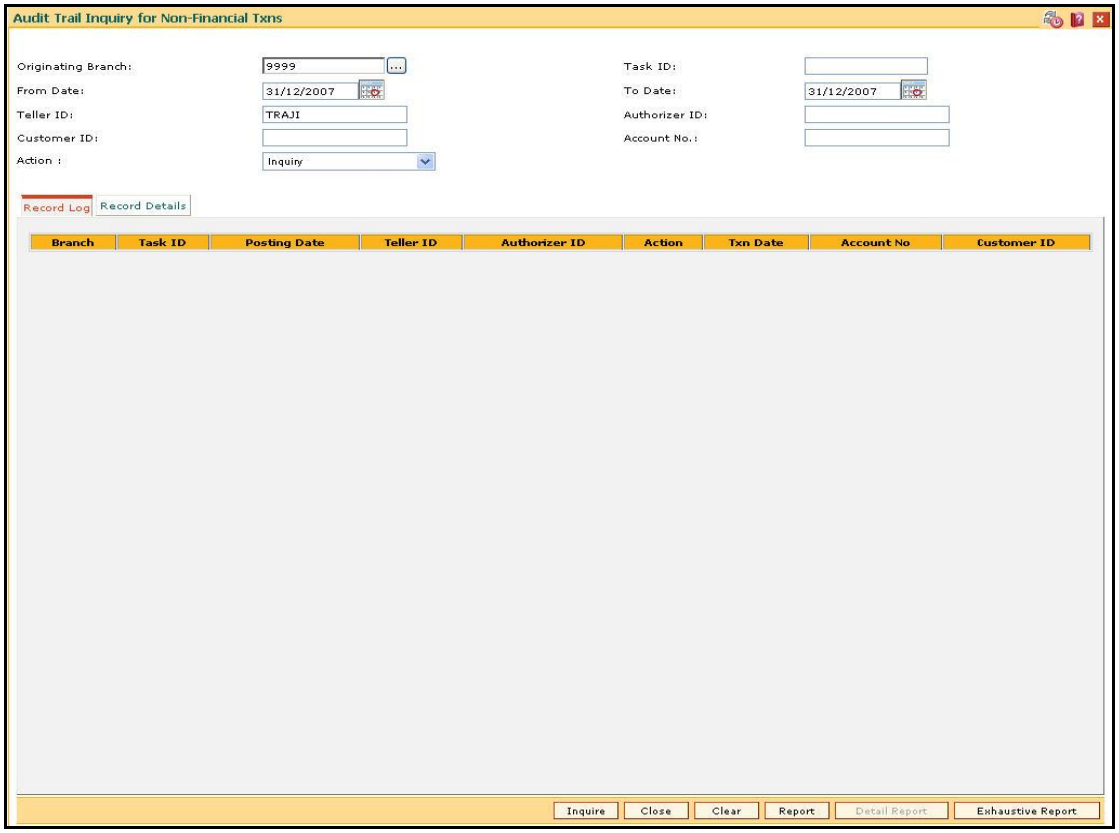
Field Description

Field Name	Description
Originating Branch	[Mandatory, Pick List] Select the originating branch, for which the audit trail is required, from the pick list.
Task ID	[Optional, Alphanumeric, Five] Type the maintenance task code being audited.
From Date	[Optional, Pick List, dd/mm/yyyy] Select the date from which the data has to be retrieved from the pick list.
To Date	[Optional, Pick list, dd/mm/yyyy] Select the date up to which the data has to be retrieved from the pick list.
Teller ID	[Optional, Alphanumeric, 16] Type the id of the teller who performed the maintenance.

Field Name	Description
Authorizer ID	[Optional, Alphanumeric, 36] Type the id of the authoriser who authorised the maintenance.
Customer ID	[Optional, Alphanumeric, 48] Type the id of the customer (if any) on whom the maintenance was done
Account No.	[Optional, Numeric, 16] Type the account number (if any) on which the maintenance was done.
Action	[Mandatory, Drop-Down] Select the maintenance action being audited from the drop-down list. The options are: • Inquiry • Add • Modify • Delete • All • All Unauthorised

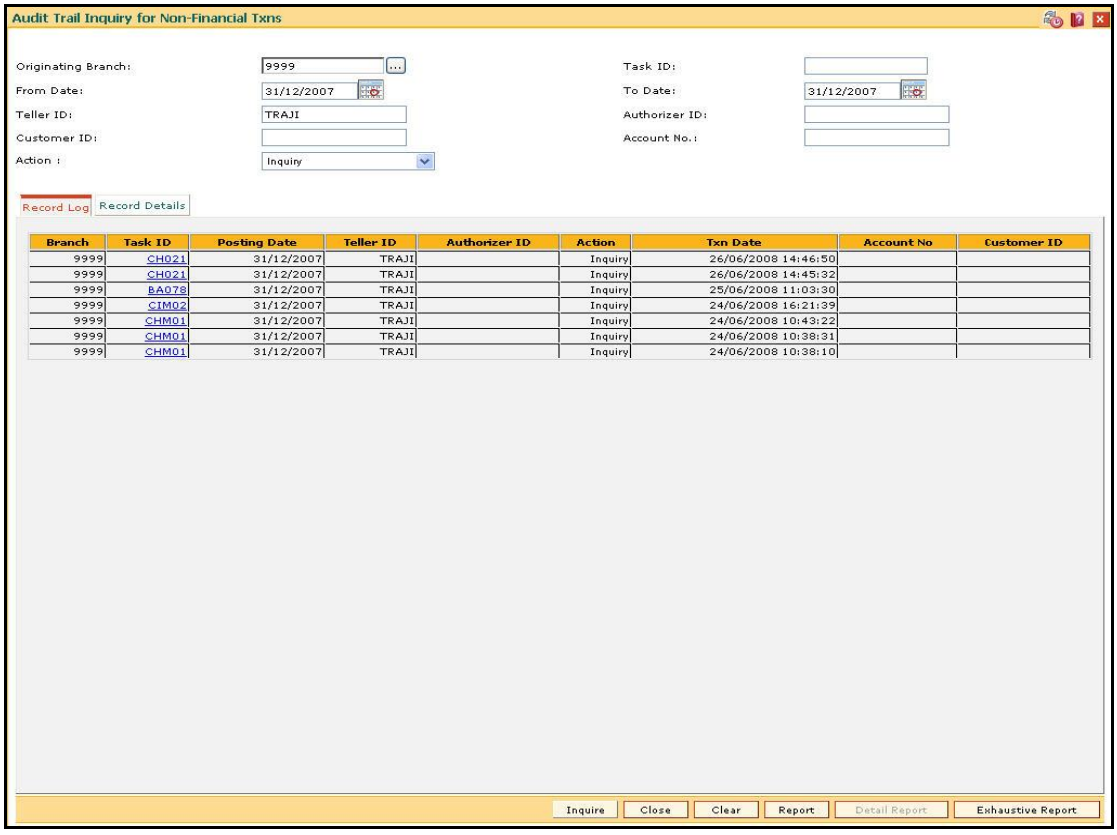
3. Select the originating branch from the pick list.
4. Enter the required information.
5. Select the action from the drop-down list.

Audit Trail Inquiry for Non-Financial Txns



6. Click the **Inquire** button.
7. The system displays the records matching the entered criteria.

Record Log


Audit Trail Inquiry for Non-Financial Txns
Originating Branch: 9999
From Date: 31/12/2007
Teller ID: TRAJI
Customer ID:
Action : Inquiry
Task ID:
To Date: 31/12/2007
Authorizer ID:
Account No.:
Record Log
Record Details
Branch | Task ID | Posting Date | Teller ID | Authorizer ID | Action | Txn Date | Account No | Customer ID
9999 | CH021 | 31/12/2007 | TRAJI | | Inquiry | 26/06/2008 14:46:50
9999 | CH021 | 31/12/2007 | TRAJI | | Inquiry | 26/06/2008 14:45:32
9999 | BA078 | 31/12/2007 | TRAJI | | Inquiry | 25/06/2008 11:03:30
9999 | CIM02 | 31/12/2007 | TRAJI | | Inquiry | 24/06/2008 16:21:39
9999 | CHM01 | 31/12/2007 | TRAJI | | Inquiry | 24/06/2008 10:43:22
9999 | CHM01 | 31/12/2007 | TRAJI | | Inquiry | 24/06/2008 10:38:31
9999 | CHM01 | 31/12/2007 | TRAJI | | Inquiry | 24/06/2008 10:38:10
Inquire
Close
Clear
Report
Detail Report
Exhaustive Report

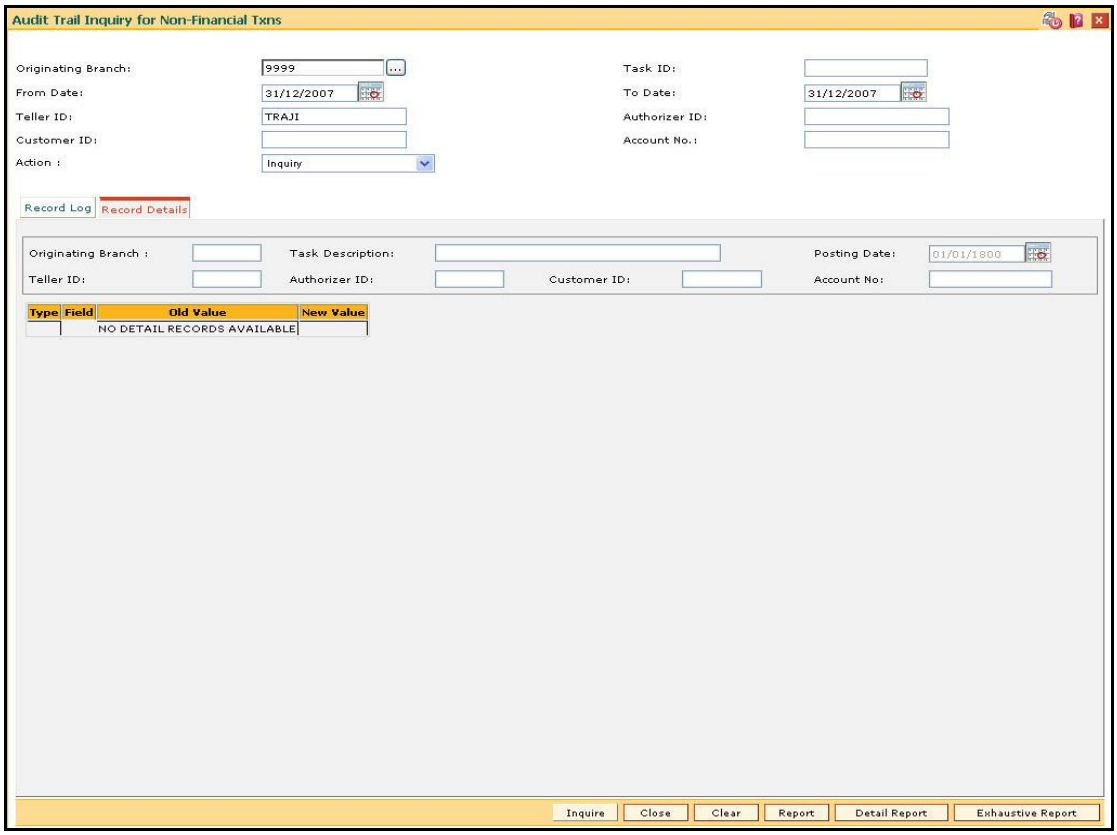
Field Description

Field Name	Description
Branch	[Display] This column displays the originating branch for which the audit trail is required.
Task ID	[Display] This column displays the maintenance task code being audited.
Posting Date	[Display] This column displays the date from which the data has to be retrieved.
Teller ID	[Display] This column displays the id of the teller who performed the maintenance.
Authorizer ID	[Display] This column displays the id of the authoriser who authorised the maintenance.

Field Name	Description
Action	[Display] This column displays the maintenance action being audited.
Txn Date	[Display] This column displays the date of transaction.
Account No	[Display] This column displays the account number (if any) on whom the maintenance was done.
Customer ID	[Display] This column displays the id of the customer (if any) on whom the maintenance was done.

8. Double-click a record to view its details in the **Record Details** tab.

Record Details



Field Description

Field Name	Description
Originating Branch	[Display] This field displays the originating branch for which the audit trail is required.
Task Description	[Display] This field displays the maintenance task description.
Posting Date	[Display] This field displays the date from which the data has to be retrieved.
Teller ID	[Display] This field displays the id of the teller who performed the maintenance.
Authorizer ID	[Display] This field displays the id of the authoriser who authorised the maintenance.
Customer ID	[Display] This field displays the id of the customer (if any) on whom the maintenance was done
Account No	[Display] This field displays the account number (if any) on whom the maintenance was done.

Column Name	Description
Type	[Display] This column indicates if this is a Key to identify the particular record in the **FLEXCUBE** database. Blank value indicates that this is not a **Key** field.
Field	[Display] This column displays the field name in the database which has changed. For a **Key** field, the actual value will also be indicated here.
Old Value	[Display] This column displays the previous value for the field being modified. This will be blank in case of **Add** option.

Column Name	Description
New Value	[Display] This column displays the new value for the field being modified. This will be blank in case of **Delete** option.

9. Reports can be executed by clicking **Report** (Only Record Log Tab), **Detailed Report** (Only Record Details Tab for a particular selection) or **Exhaustive Report** (Complete details of all Record Log records).
10. Click the **Close** button.

Note: The report output can then be viewed by navigating to the **Advice/Report Status Inquiry** option (Fast Path: 7778).

1.14. BAM04 - BA Audit Tasks Maintenance-Inquire

Using this option you can decide the auditing matrix for a particular task. This option can be used to define whether an audit is allowed on a maintenance option, and the actions (add, modify, delete, etc.) from that window should be recorded in an audit log.

All online transactions with financial impact except for Voucher Entry transaction are recorded in the Electronic Journal (EJ) stored at the respective branch. This maintenance is used for auditing all the other transactions. The audit log is stored in the central host and is common to all the branches.

Definition Prerequisites

- BAM15 - Transaction Mnemonic Codes

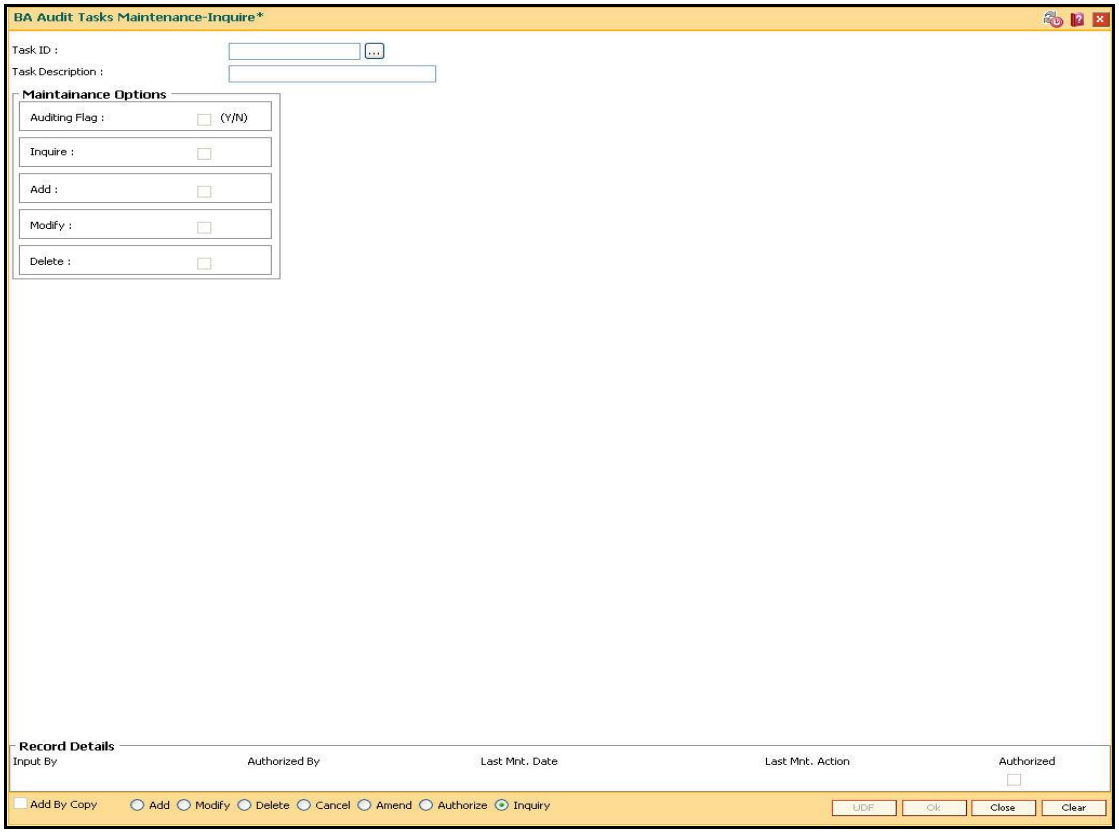
Modes Available

Add By Copy, Add, Modify, Delete, Cancel, Amend, Authorize, Inquiry. For more information on the procedures of every mode, refer to **Standard Maintenance Procedures**.

To add audit task details

1. Type the fast path **BAM04** and click **Go** or navigate through the menus to **Global Definitions > Other > BA Audit Tasks Maintenance-Inquire**.
2. The system displays the **BA Audit Tasks Maintenance-Inquire** screen.

BA Audit Tasks Maintenance-Inquire



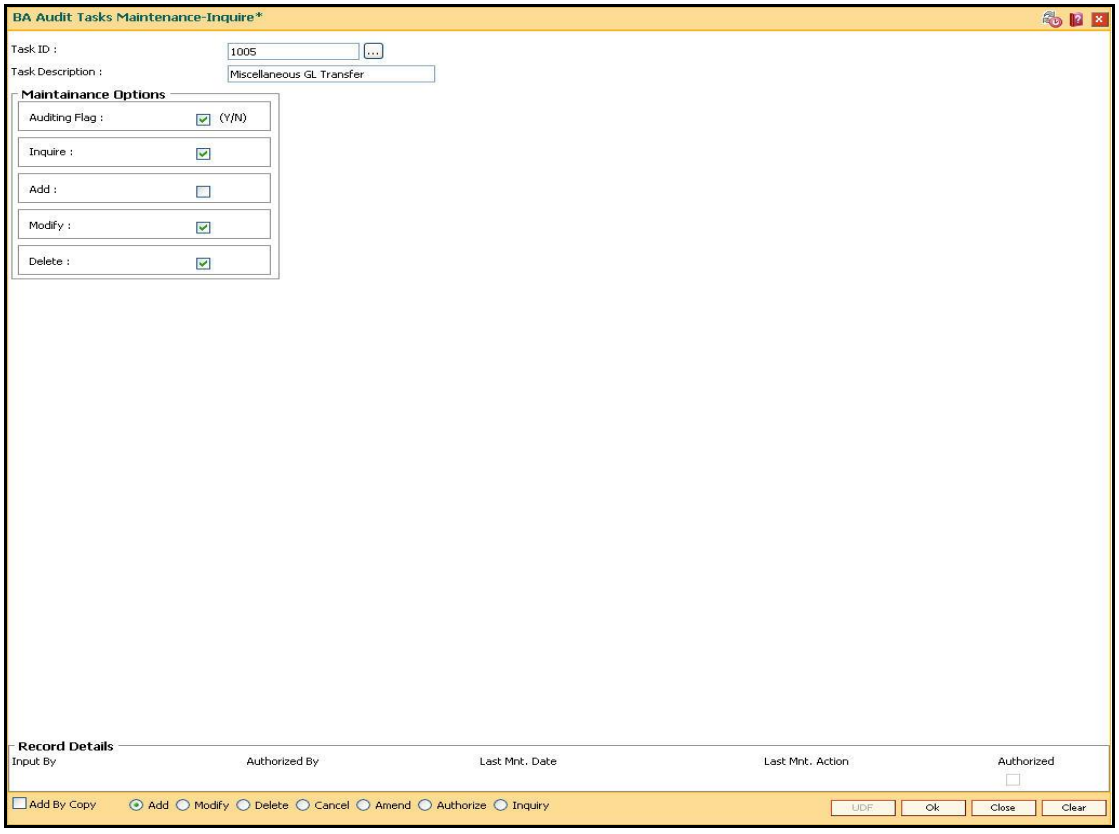
Field Description

Field Name	Description
Task ID	[Mandatory, Pick List] Select the task ID from the pick list. Task ID lists all the transaction codes maintained in the **Transaction Mnemonic Codes** (Fast Path: BAM15) option. This ID acts like a fast path. The fast path is a mnemonic which allows the user to access the options.
Task Description	[Display] This field displays the description of the selected task code.
Maintenance Options	
Auditing Flag	[Mandatory, Check Box] Select the Auditing Flag check box, to enable the auditing flag. If the check box is selected, the details of the transaction will be recorded and stored for audit purposes. The maintenance options will also be enabled if the auditing flag is selected.
Inquire	[Conditional, Check Box] Select the Inquire check box, if you want the system to record the inquire actions and store the same for audit purposes. If the **Inquire** check box is selected it enables you to inquire about an authorised record. This field is enabled only if the **Auditing Flag** check box is selected.
Add	[Conditional, Check Box] Select the Add check box to enable you to add a new record to the selected task id. If the **Add** check box is selected, the system records the add actions and stores the same for audit purposes. This field is enabled only if the **Auditing Flag** check box is selected.
Modify	[Conditional, Check Box] Select the **Modify** check box to enable you to modify a record in the selected task id. If the Modify check box is selected, the system records the modify actions and stores the same for audit purposes. This field is enabled only if the **Auditing Flag** check box is selected.

Field Name	Description
Delete	[Conditional, Check Box] Select the Delete check box to enable you to delete a record from the selected task id. If the **Delete** check box is selected, the system records the delete actions and stores the same for audit purposes. This field is enabled only if the **Auditing Flag** check box is selected.

3. Click the **Add** button.
4. Select the task ID from the pick list.
5. Select the auditing flag check box and the appropriate maintenance option check boxes.

BA Audit Tasks Maintenance-Inquire



6. Click the **Ok** button.
7. The system displays the message "Record Added...Authorisation Pending..Click Ok to Continue". Click the **OK** button.
8. The audit task is added once the record is authorised.

1.15. BAM10 - Restricted Accounts Maintenance

Using this option you can restrict a particular teller from accessing the details of particular customer or GL accounts.

For example: If the bank decides to restrict the access to income and expenses accounts this option can be used. For a restricted account, the teller is not allowed to post any transaction, inquire, or maintain details.

Definition Prerequisite

- SMM02 - User Profile Maintenance

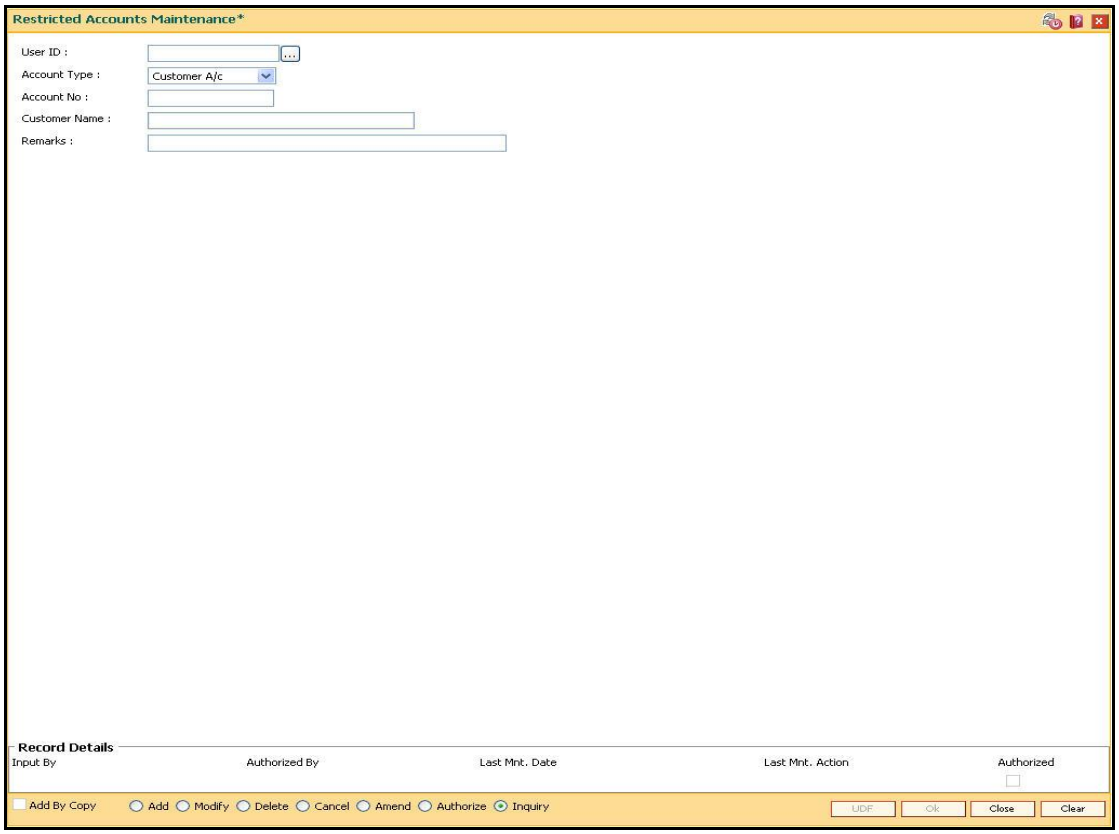
Modes Available

Add By Copy, Add, Modify, Delete, Cancel, Amend, Authorize, Inquire. For more information on the procedures of every mode, refer to **Standard Maintenance Procedures**.

To add a teller restricted account

1. Type the fast path **BAM10** and click **Go** or navigate through the menus to **Transaction Processing > Internal Transactions > Others > Restricted Accounts Maintenance**.
2. The system displays the **Restricted Accounts Maintenance** screen.

Restricted Accounts Maintenance

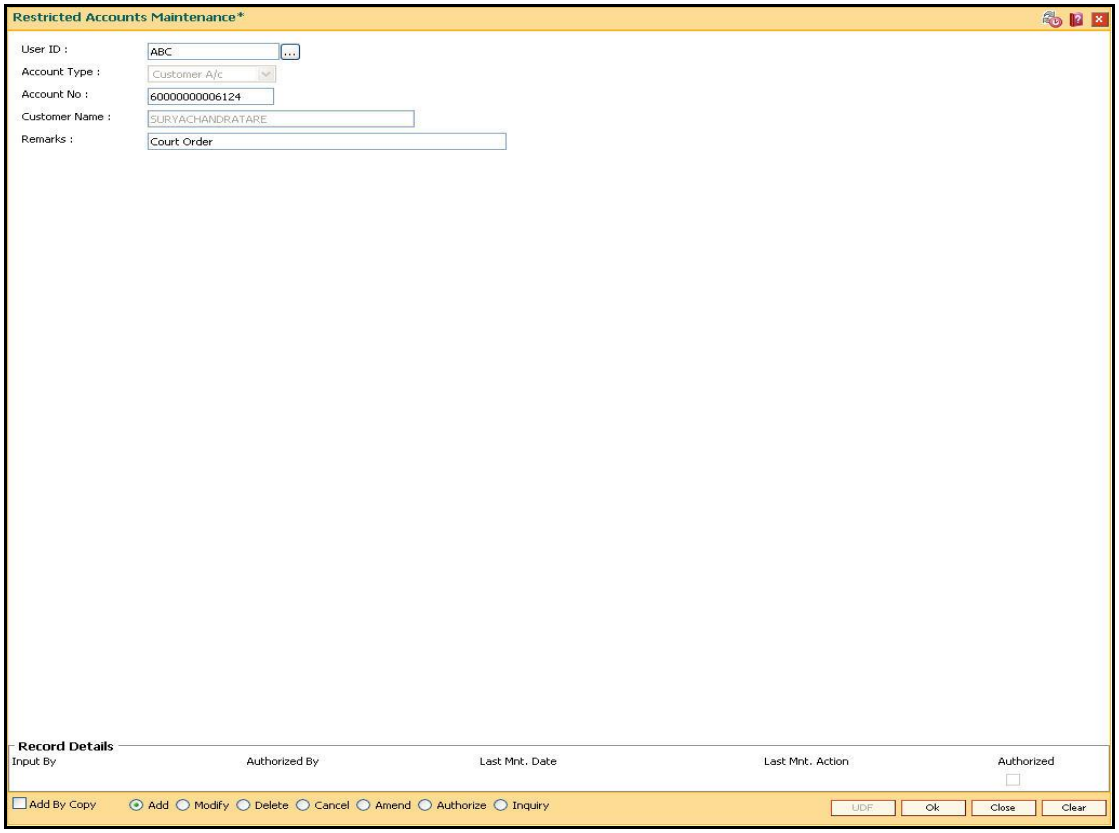


Field Description

Field Name	Description
User ID	[Mandatory, Pick List] Select the user ID from the drop-down list. These user IDs are added and maintained in the **Defining User Profile** (Fast Path: SMM02) option. Once added, this field cannot be modified or amended.
Account Type	[Mandatory, Drop-Down] Select the account type on which restriction is to be imposed from the drop-down list. The options are: • Customer A/C: It enables the **Account No** field in which you enter the customer account number. • General Ledger A/C: It enables the **Account No** field in which you enter the GL account number. Once added, this field cannot be modified or amended.
Account No	[Mandatory, Alphanumeric, 16] Type the account number based on the selected account type. The system does not validate the status of the account.
Customer Name	[Display] This field displays the name of the customer if you select the **Customer A/C** option from the **Account Type** drop-down list.
Remarks	[Optional, Alphanumeric, 40] Type the reason for the restriction. This is for information purposes only.

3. Click the **Add** button.
4. Select the user ID from the pick list and the account type from the drop-down list.
5. Enter the account number and press the <**Tab**> key.

Restricted Accounts Maintenance



6. Click the **OK** button.
7. The system displays the message "Record Added...Authorisation Pending...". Click the **OK** button.
8. The teller restricted account is added once the record is authorised.

1.16. SM11A - Inquiry On Logged In Users

Using this option you can view the status of the currently logged in users for all the branches. The system provides information on user ID, user name, branch code and the terminal ID in which the user has logged in and the login date and time. You can refresh the screen to get the latest status.

Definition Prerequisites

- SMM02 - User Profile Maintenance

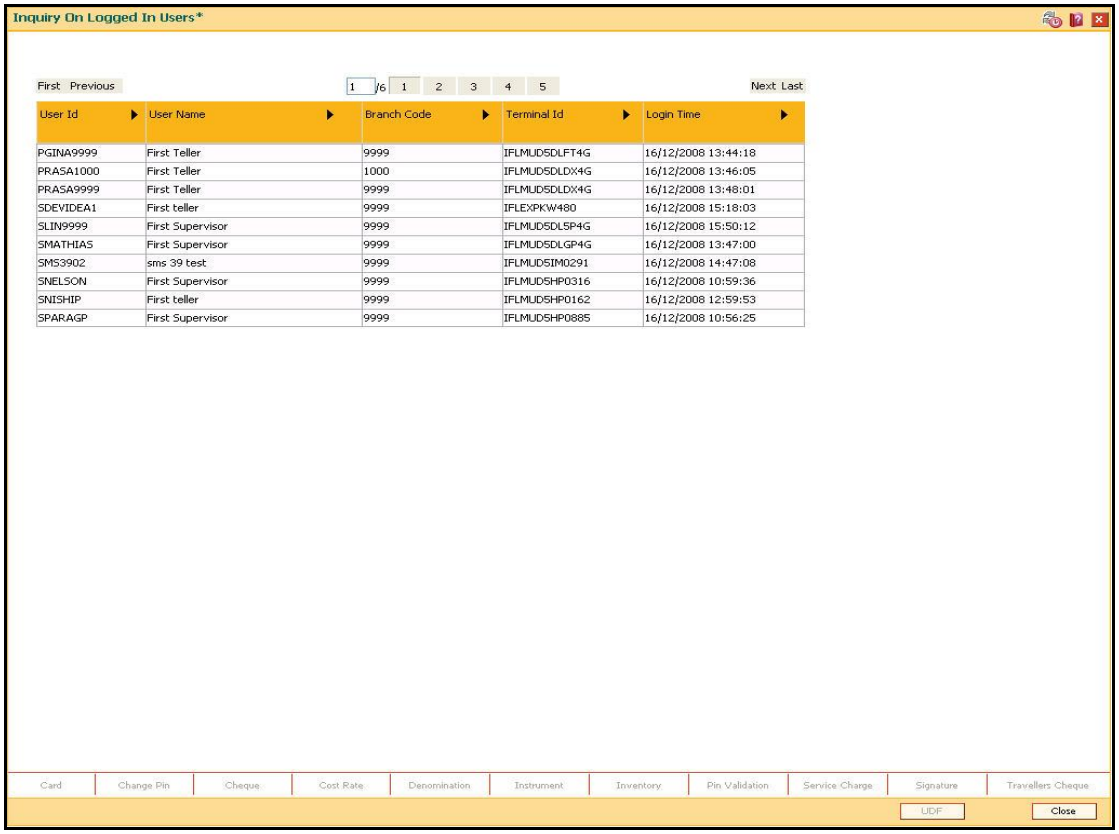
Modes Available

Not Applicable

To inquiry on logged in users

1. Type the fast path **SM11A** and click **Go** or navigate through the menus to **Global Definitions > Security > Inquiry On Logged In Users**.
2. The system displays the **Inquiry On Logged In Users** screen.

Inquiry On Logged In Users



Field Description

Column Name	Description
User Id	[Display] This column displays the user ID.
User Name	[Display] This column displays the name of the user, based on the user ID.
Branch Code	[Display] This column displays the branch code to which the logged in users belong to.
Terminal Id	[Display] This column displays the identification code of the terminal where each user has logged in to the system.
Login Time	[Display] This column displays the date and time on which the user had last logged in.

3. Click the **Close** button.

1.17. SMM02 - User Profile Maintenance

Using this option you can add user profiles centrally for a new user to be created in the system. In User Profile Maintenance, various attributes and roles of a user are defined.

Using the **Modify User Details** tab, you can maintain the Resetting of Primary Password, Primary Password Expiry Date change, Modification in Login Status and Enable/Disable User.

Definition Prerequisites

- SMM18 - Access Domain Maintenance
- SMM14 - Template Securities Settings

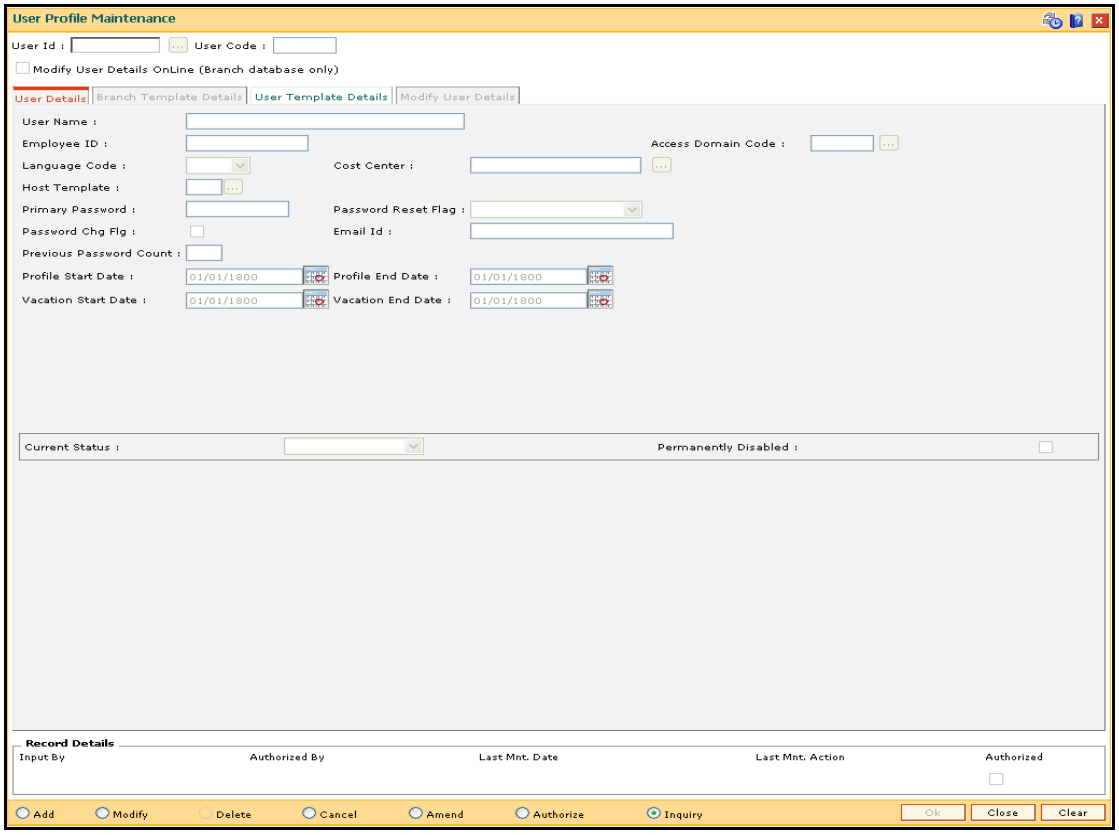
Modes Available

Add, Modify, Cancel, Amend, Authorize, Inquiry. For more information on the procedures of every mode, refer to **Standard Maintenance Procedures**.

To add the user profile details

1. Type the fast path **SMM02** and click **Go** or navigate through the menus to **Global Definitions > Security > User Profile Maintenance**.
2. The system displays the **User Profile Maintenance** screen.

User Profile Maintenance

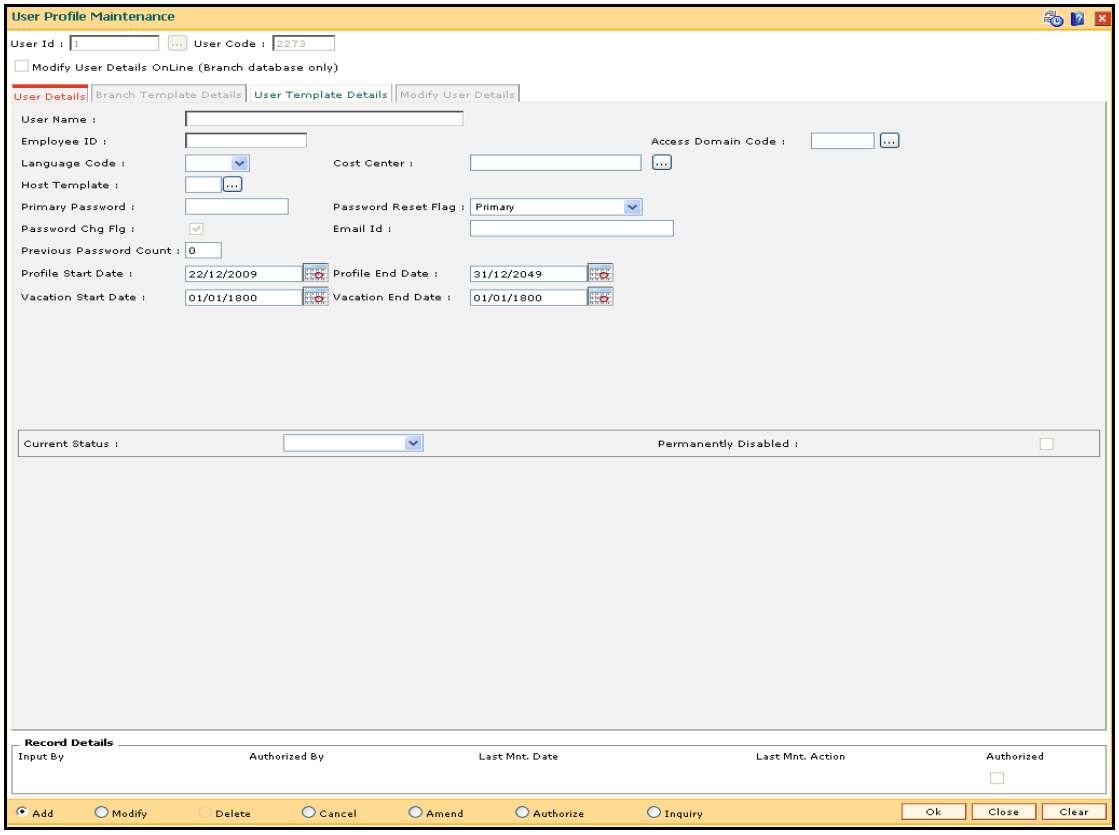


Field Description

Field Name	Description
User Id	[Mandatory, Alphanumeric, 12] Type the identification code for the user.
User Code	[Display] This field displays the system-generated user code.
Modify User Details OnLine (Branch database only)	[Conditional, Check Box] Select the **Modify User Details OnLine (Branch database only)** check box to modify the user details. This field is enabled in the **Modify** mode. Selecting this check box enables the **Modify User Details** tab. This option is used if there is a centralized system administrator so that the administrator can change the following details for any user of any branch. • Reset Primary Password • Change Primary Password Expiry Date • Modify Login Status • Enable/Disable User

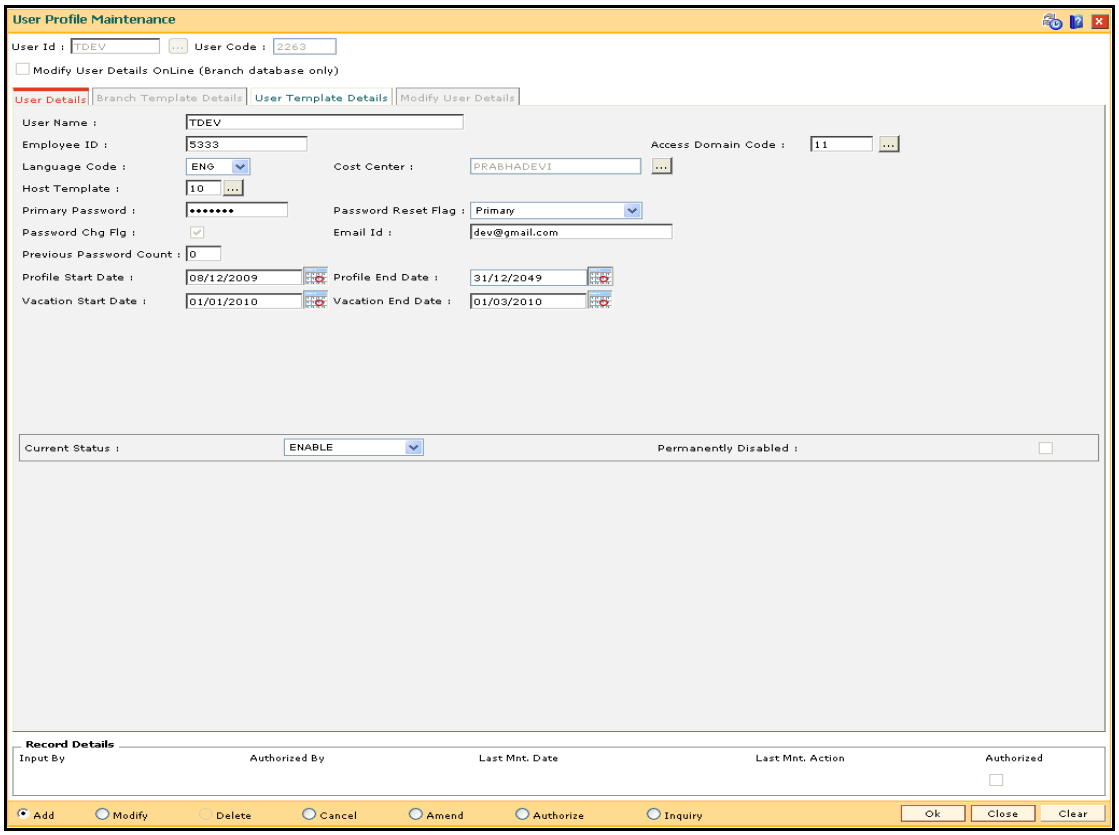
3. Click the **Add** button.
4. Type the user ID and press the **<Tab>** key.

User Profile Maintenance



5. Modify the required information in the various tab screens.

User Details



Field Description

Field Name	Description
User Name	[Mandatory, Alphanumeric, 40] Type the name of the user. It should be unique for all branches. This field cannot be modified or amended.
Employee ID	[Mandatory, Alphanumeric, 40] Type the employee ID of the bank staff.
Access Domain Code	[Mandatory, Pick List] Select the appropriate access domain code from the pick list. The access domain codes are maintained in the **Access Domain Maintenance** (Fast Path: SMM18)option. Based on the access domain and access codes, the user will be able to inquire and maintain accounts that are having one of the access code included in the users access domain or else the inquiry/maintenance will not be allowed for that user on that CIF/Account.

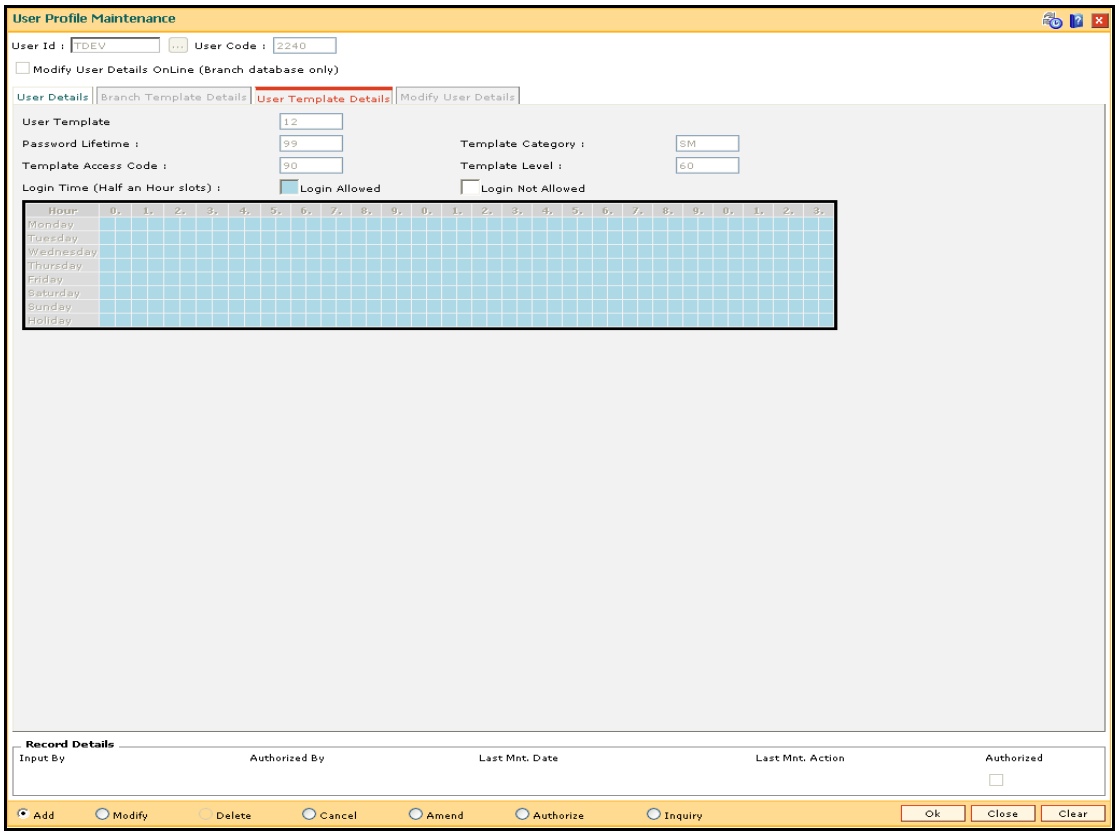
Field Name	Description
Language Code	[Mandatory, Drop-Down] Select the code of the language from the drop-down list.
Cost Center	[Mandatory, Pick List] Select the branch code of the user from the pick list.
Host Template	[Mandatory, Pick List] Select the code of the host template from the pick list. If the field is blank, the value of the template is taken as zero and the user is attached only to the host template.
Primary Password	[Mandatory, Alphanumeric, 12] Type the primary password. Password policy of the bank can be set at the template level by **Template Security Settings** (Fast Path: SMM14). For e.g., It should be a combination of an uppercase and lowercase letter, and a numeric digit. This field cannot be modified or amended. The value can be between eight and 12.
Password Reset Flag	[Optional, Drop-Down] Select the password reset flag from the drop-down list. The options are: • Primary • Secondary • Both • None When the user logs in for the first time, a password change would be required if any option other than **None** is selected. This field cannot be modified or amended.
Password Chg Flg	[Display] This field is selected if the change in password is required during the first login.
Email Id	[Mandatory, Alphanumeric, 60] Type the e-mail address of the user.
Previous Password Count	[Mandatory, Numeric, One] Type the number of previous passwords that cannot be used again. This field cannot be modified or amended.
Profile Start Date	[Mandatory, Pick List, dd/mm/yyyy] Select the date from which the user's profile will be enabled from the pick list. This field cannot be modified or amended.

Field Name	Description
Profile End Date	[Mandatory, Pick List, dd/mm/yyyy] Select the date after which the user's profile will no longer be valid from the pick list.
Vacation Start Date	[Mandatory, Pick List, dd/mm/yyyy] Select the vacation start date from the pick list. The user cannot access the system during the specified vacation period. This ensures that any illegal attempt to access the system is not allowed. The system validates between the vacation start date and vacation end date (Excluding both the dates). This date should be later than the profile start date. This field cannot be modified or amended.
Vacation End Date	[Mandatory, Pick List, dd/mm/yyyy] Select the vacation end date from the pick list. The user can access the system when he or she returns from the vacation. The system validates between the vacation start date and vacation end date (Excluding both the dates). This date should be before the profile end date. This field cannot be modified or amended.
Current Status	[Mandatory, Drop-Down] Select the current status of the user from the drop-down list. The options are: • Disable • Enable • Lock
Permanently Disabled	[Display] This field displays the status of the user. The check box is selected if the user is permanently disabled.

Branch Template Details

This tab is for future use.

User Template Details



Field Description

Field Name	Description
User Template	[Display] This field displays the template code of the template linked to the user. Each code uniquely identifies a different template.
Password Lifetime	[Display] This field displays the password validity period for the user.
Template Category	[Display] This field displays the category of the template. The category identifies the role of the user, whether the user is the security manager, system operator or other user.

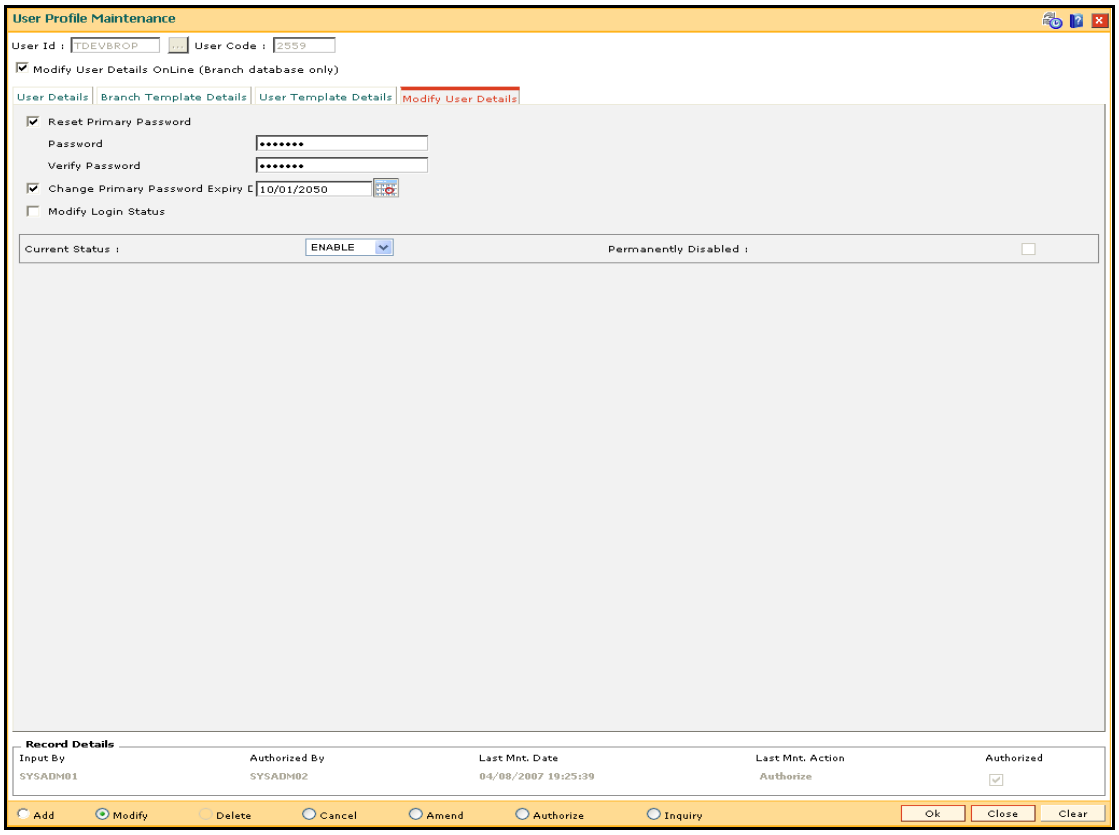
Field Name	Description
Template Access Code	[Display] This field displays the access code of the template. It indicates the type of accounts in the bank that the users of a given template can access.
Template Level	[Display] This field displays the level of the template. It indicates the authority of the user. The higher the template level, the higher is the user's profile.
Login Time (Half an Hour slots)	[Display] This field displays the login time of the user. The user can log into the system only during specified slots during the week. The duration of each slot is half an hour. The options are: • Login Allowed (Light Blue): Indicates that the user has access to the system during that time slot. • Login Not Allowed (White): Indicates that the user does not have access to the system during that time slot.

6. Click the **Ok** button.
7. The system displays message "Record Added...Authorisation Pending...Click Ok to Continue". Click the **OK** button.
8. The user profile details are added once the record is authorized.

To modify the user profile details

1. Click the **Modify** button.
2. Select the user ID from the pick list.
3. To modify the user details online, select the **Modify User Details Online** check box.
4. The system displays the **Modify User Details** tab.

Modify User Details



Field Description

Field Name	Description
Reset Primary Password	[Optional, Check Box] Select the **Reset Primary Password** check box to reset the primary password.
Password	[Conditional, Alphanumeric, 12] Type the new password for the user. It should be a combination of an uppercase and lowercase letter and a numeric digit. The password cannot have three or more successive characters or digits. For example, abc, xyz, etc. The value can be between eight and 12. This field is enabled only if the **Reset Primary Password** check box is selected.

Field Name	Description
Verify Password	[Conditional, Alphanumeric, 12] Type the new password to verify it. This field is enabled only if the **Reset Primary Password** check box is selected.
Change Primary Password Expiry Date	[Optional, Check Box] Select the **Change Primary Password Expiry Date** check box to change the user's primary password expiry date. [Conditional, Pick List, dd/mm/yyyy] Select the date on which the primary password will expire from the pick list. This field is enabled only if the **Change Primary Password Expiry Date** check box is selected.
Modify Login Status	[Optional, Check Box] Select the **Modify Login Status** check box to modify the user login status.
Current Status	[Mandatory, Drop-Down] Select the current status of the user from the drop-down list. The options are: • Disable • Enable • Lock
Permanently Disabled	[Optional, Check Box] Select this check box to permanently disable a user id.

5. Click the **Ok** button.
6. The system displays message "Record Modified...Authorization Pending...Click Ok to Continue". Click the **OK** button.
7. The user profile details are modified once the record is authorised.

1.18. SMM03 - Task Profile Maintenance

Using this option you can maintain a task profile which includes the following details like Task ID, Task Description and Category.

All options are broken into tasks that can be individually assigned to the user. You can use a task only if you have access rights to it. A group of tasks in conjunction will display a menu with options that lead to screens. Depending on the tasks assigned , the menus are generated dynamically. Each task has a task profile associated with it.

Definition Prerequisites

- BAM15 - Transaction Mnemonic Codes

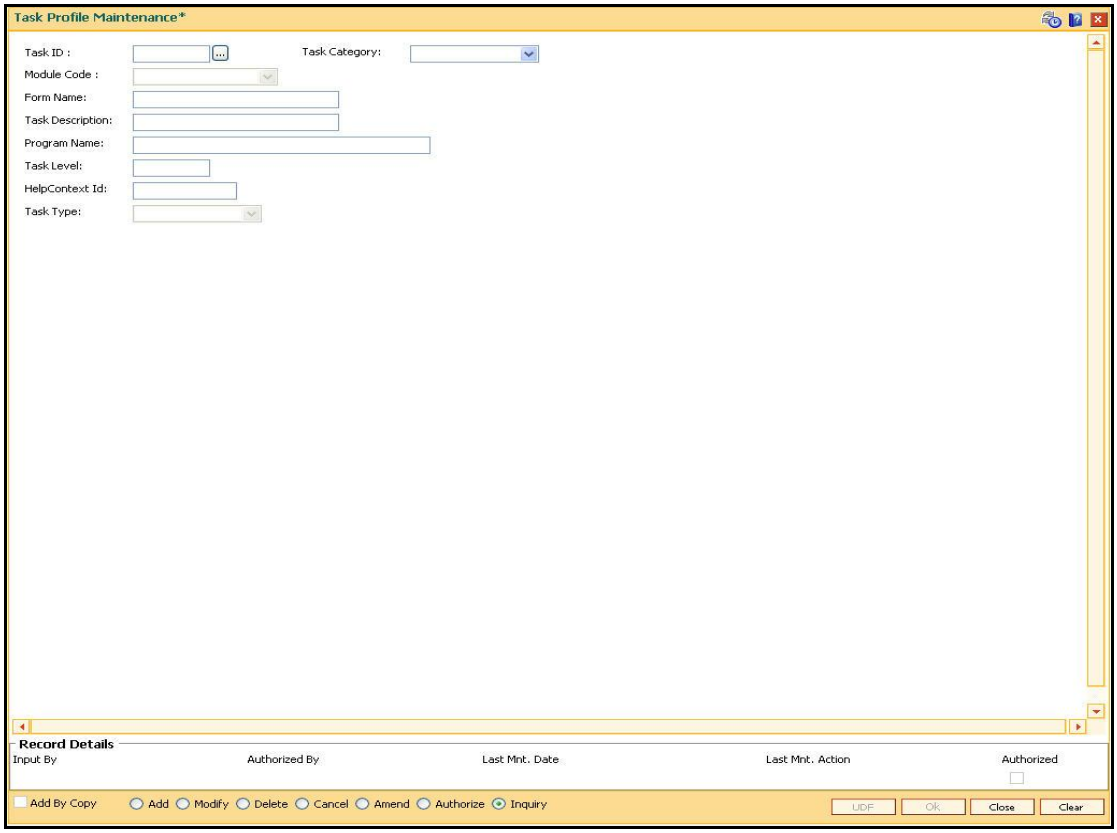
Modes Available

Add By Copy, Add, Modify, Delete, Cancel, Amend, Authorize, Inquiry. For more information on the procedures of every mode, refer to **Standard Maintenance Procedures**.

To add the task profile details

1. Type the fast path **SMM03** and click **Go** or navigate through the menus to **Global Definitions > Security > Task Profile Maintenance**.
2. The system displays the **Task Profile Maintenance** screen.

Task Profile Maintenance



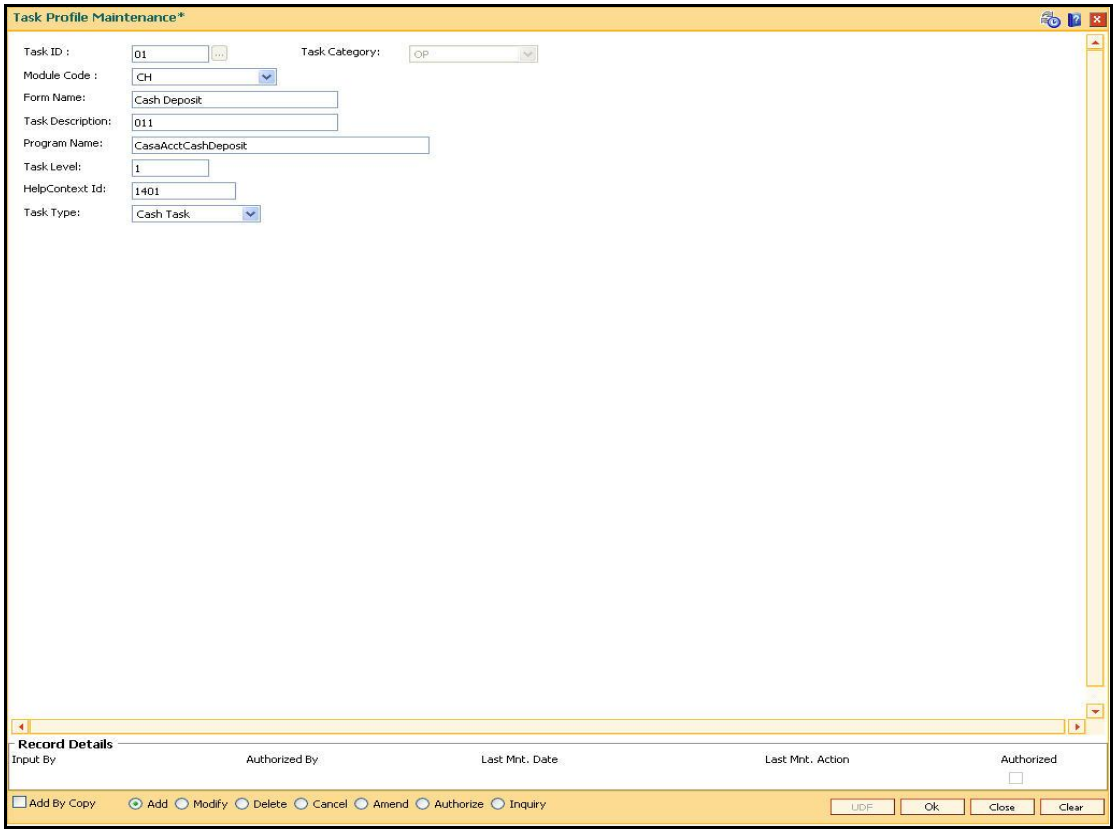
Field Description

Field Name	Description
Task ID	[Mandatory, Alphanumeric, Five] Type the appropriate task code. The task codes are assigned to the tasks or type of transactions that the user can access. Task code is a unique ID assigned to maintenance to provide easy access to the users. Once added, this field cannot be modified.
Task Category	[Mandatory, Drop-Down] Select the task category from the drop-down list. The options are: • OP (Operator) - The System Operators are the other users of **FLEXCUBE** Retail application. The responsibility of system operators includes: End of Day Processing, File Transfer, Archival/Retrieval. The System Operators cannot perform any application related activities. • OT (Other Tellers) - The Other Tellers are the on-line users. They have the maximum interaction with **FLEXCUBE Retail** application. The responsibility of other tellers includes: Tables Maintenance, Performing Host transactions. This category of users cannot perform any System Administrator / System Operator kind of activities. These users perform all the application related activities • SM (Security Manager) - The security manager has management level access rights. The responsibility of Security Manager includes: User Profile Maintenance, Template Profile Maintenance, Class Profile Maintenance, User Class Linkage, Task Access Control, System Security (involving Audit trail tracking and Exception activities tracking). The Security Manager cannot perform any application related activities. It indicates that the user with specific access rights can perform the assigned task.
Module Code	[Mandatory, Drop-Down] Select the code of the module to which the task ID belongs from the drop-down list. The user can maintain a sequence format that will be applicable to all the modules available in the bank.
Form Name	[Optional, Alphanumeric, 30] Type the DLL name of the related function. This field is currently not in use.
Task Description	[Mandatory, Alphanumeric, 40] Type the description for the task that the user wants to add.

Field Name	Description
Program Name	[Optional, Alphanumeric, 64] Type the name of the program, which is linked to the parent task. The name of the program cannot begin with underscore. This field has to be blank if the process code is blank.
Task Level	[Mandatory, Numeric, Four] Type the level of the task. All templates with a level greater than the specified level can be granted access to this task.
HelpContext Id	[Optional, Numeric, Nine] Type the help context identification number of the task.
Task Type	[Optional, Drop-Down] Select the task type from the drop-down list. The options are: • Cash Task • Non-Cash Task

3. Click the **Add** button.
4. Enter the task id and select the task category from the drop-down list.
5. Select the module code from the drop-down list.
6. Enter the form name, task description, program name, and help context id.

Task Profiles Maintenance



7. Click the **Ok** button.
8. The system displays message "Record Added...Authorisation Pending...Click Ok to Continue". Click the **OK** button.
9. The task profile is added once the record is authorized.

1.19. SMM09 - User Prohibited Password Maintenance

Security Management System can maintain two lists of passwords that each user should not use. One list is common to all users in the branch, and the other is unique to each user.

Using this option you can maintain a list of prohibited passwords for each user individually. These passwords are generally names, words, and numbers that can be easily associated with the user. For example, name of the user's spouse, car number, telephone number, date of birth, etc. When a new user is added to the system, a new list of user prohibited passwords can be added.

Definition Prerequisites

- User Ids to be available for this maintenance

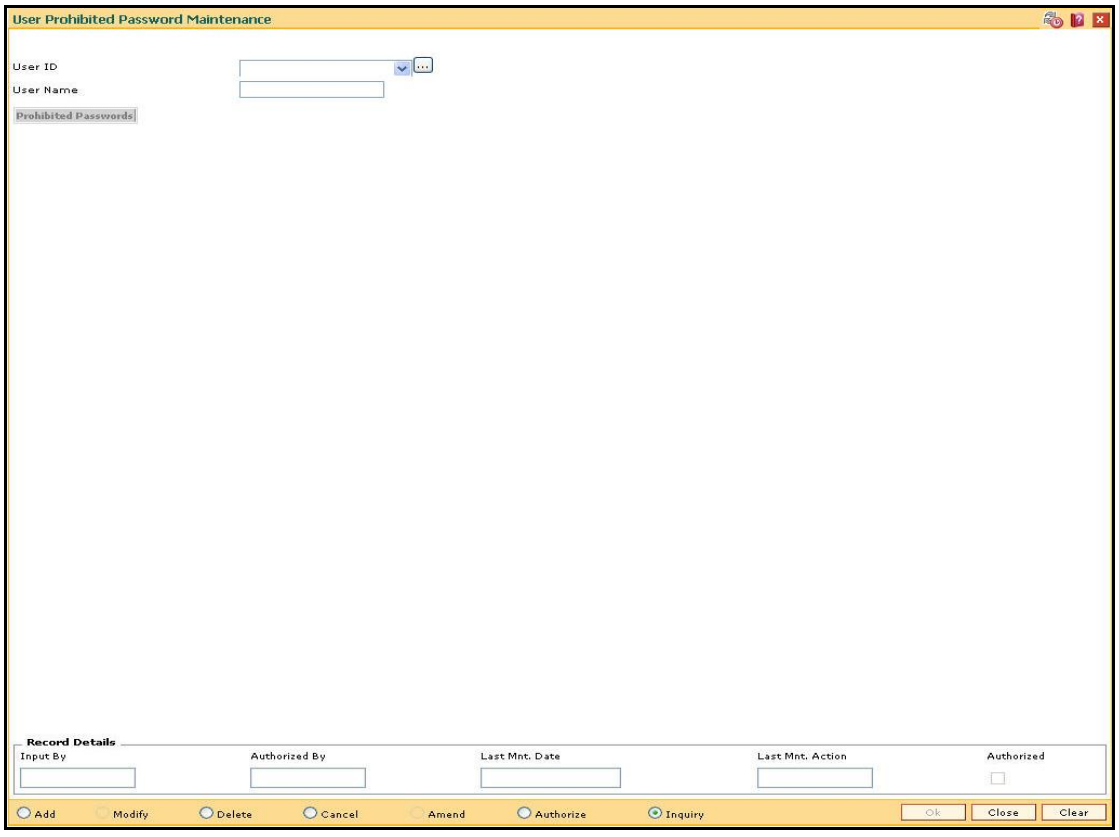
Modes Available

Add, Delete, Cancel, Authorize, Inquiry. For more information on the procedures of every mode, refer to **Standard Maintenance Procedures**.

To add user prohibited passwords

1. Type the fast path **SMM09** and click **Go** or navigate through the menus to **Transaction Processing > Internal Transactions > Others > User Prohibited Password Maintenance**.
2. The system displays the **User Prohibited Password Maintenance** screen.

User Prohibited Password Maintenance

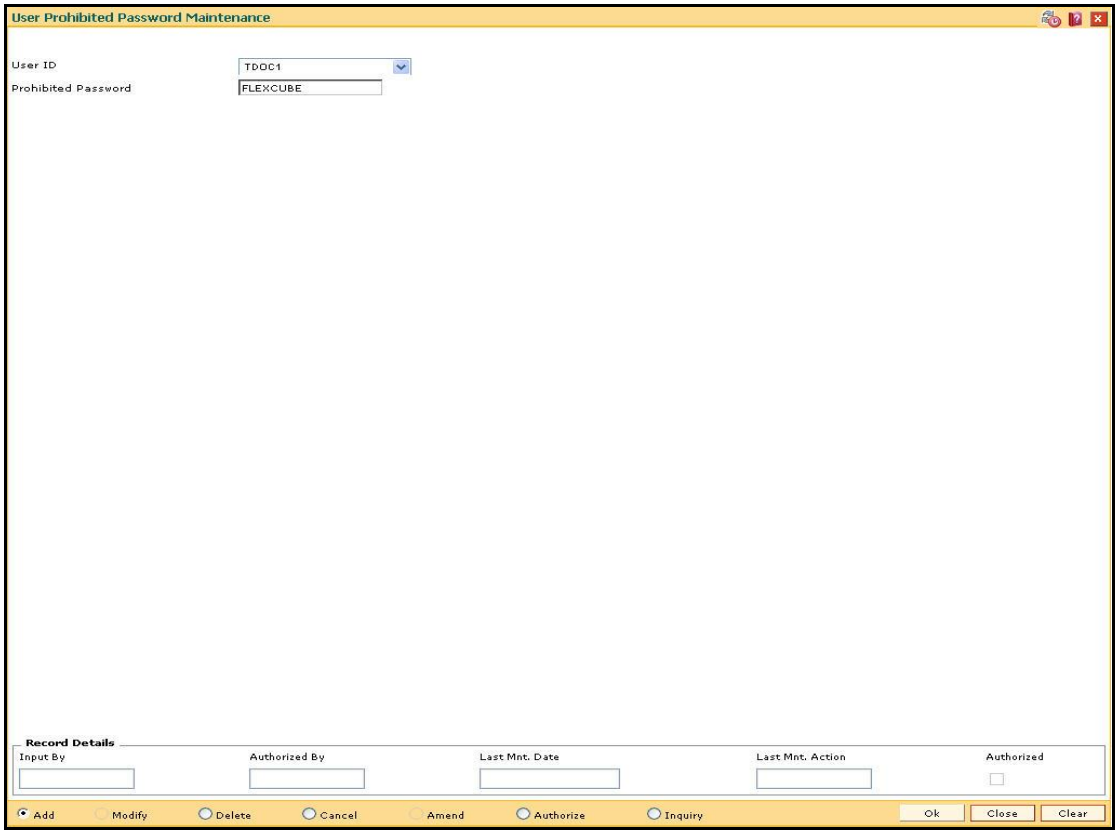


Field Description

Field Name	Description
User ID	[Mandatory, Drop-Down] Select the ID of the user, to add a list of prohibited passwords, from the drop-down list.
User Name	[Display] This field displays the user name of the Id selected in the corresponding field.
Prohibited Passwords	[Mandatory, Alphanumeric, 12] Type the password that is prohibited for this user ID.

3. Click the **Add** button.
4. Select the user Id from the drop-down list.
5. Enter the password that is prohibited for this user.

User Prohibited Password Maintenance

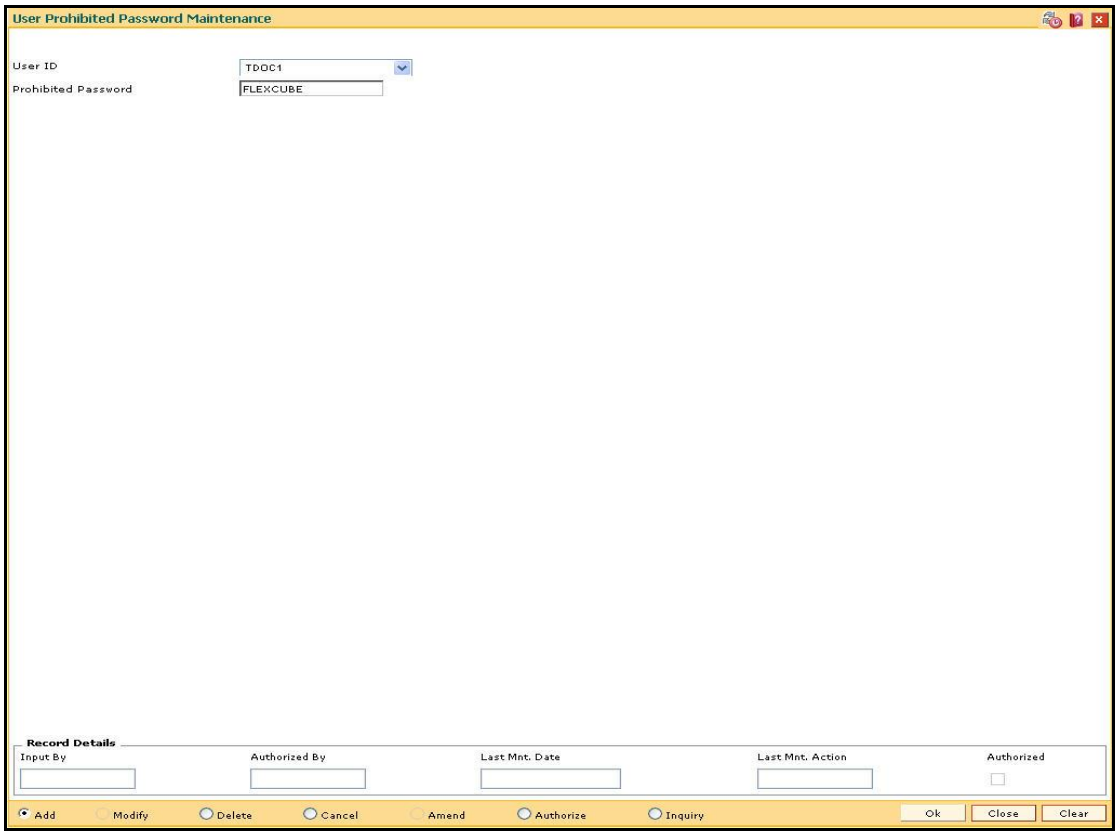


6. Click the **Ok** button.
7. The system displays the message "Record Added ...Authorisation Pending. Click Ok to Continue". Click the **OK** button.
8. The prohibited password gets added once the record is authorised.

To view the user prohibited passwords

1. Click the **Inquiry** button.
2. Select the user id from the drop-down list.
3. The system displays the list of prohibited passwords for the selected user.

User Prohibited Password Maintenance



4. Click the **Close** button**.**

1.20. SMM12 - User Class Cross Reference Maintenance

Classes are created for grouping users for authorisation purposes. Any action performed by the maker of a particular class, will have to be authorised by the authoriser of the same class. A user can be linked to more than one class.

Users in the branch are given access to various classes maintained in the **Class Profile Maintenance** (Fast Path: SMM04) option. Using this option allows the system administrator to enable users to belong to various pre-defined classes.

Definition Prerequisite

- SMM02 - User Profile Maintenance
- SMM04 - Class Profile Maintenance

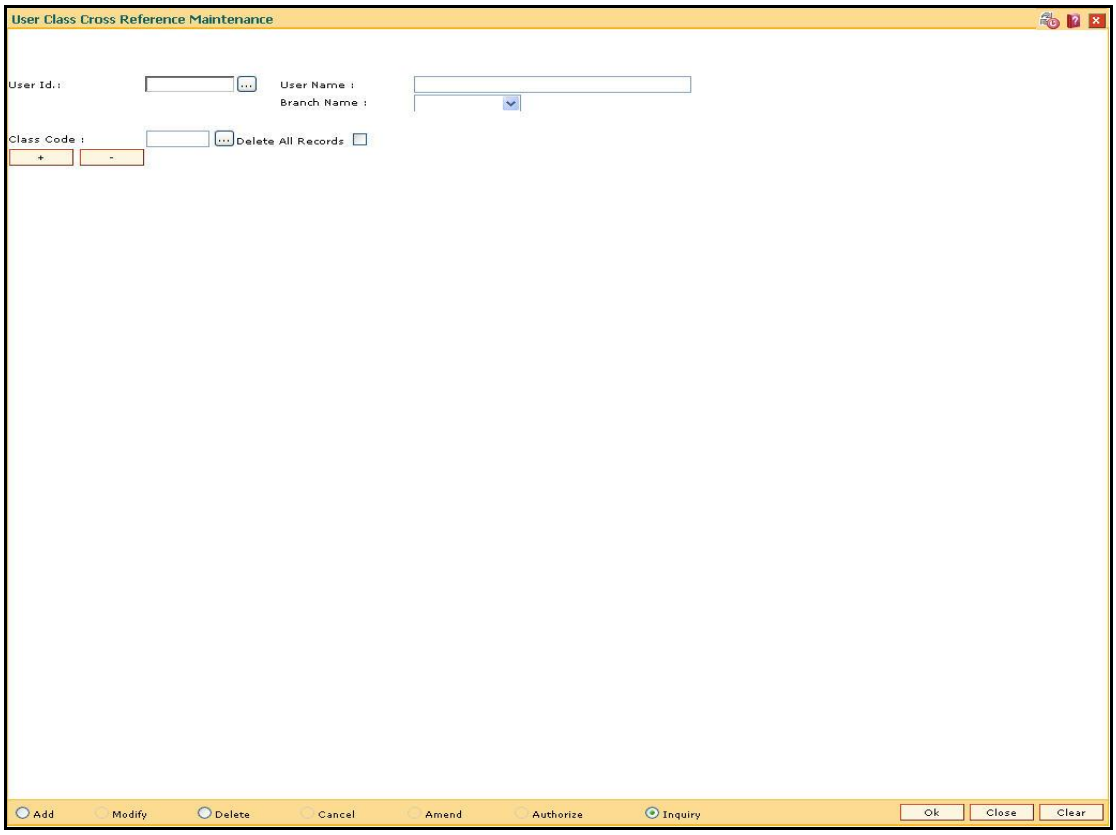
Modes Available

Add, Delete, Inquire. For more information on the procedures of every mode, refer to **Standard Maintenance Procedures**.

To add a user class cross reference

1. Type the fast path **SMM12** and click **Go** or navigate through the menus to **Global Definitions > Security > User Class Cross Reference Maintenance**.
2. The system displays the **User Class Cross Reference Maintenance** screen.

User Class Cross Reference Maintenance



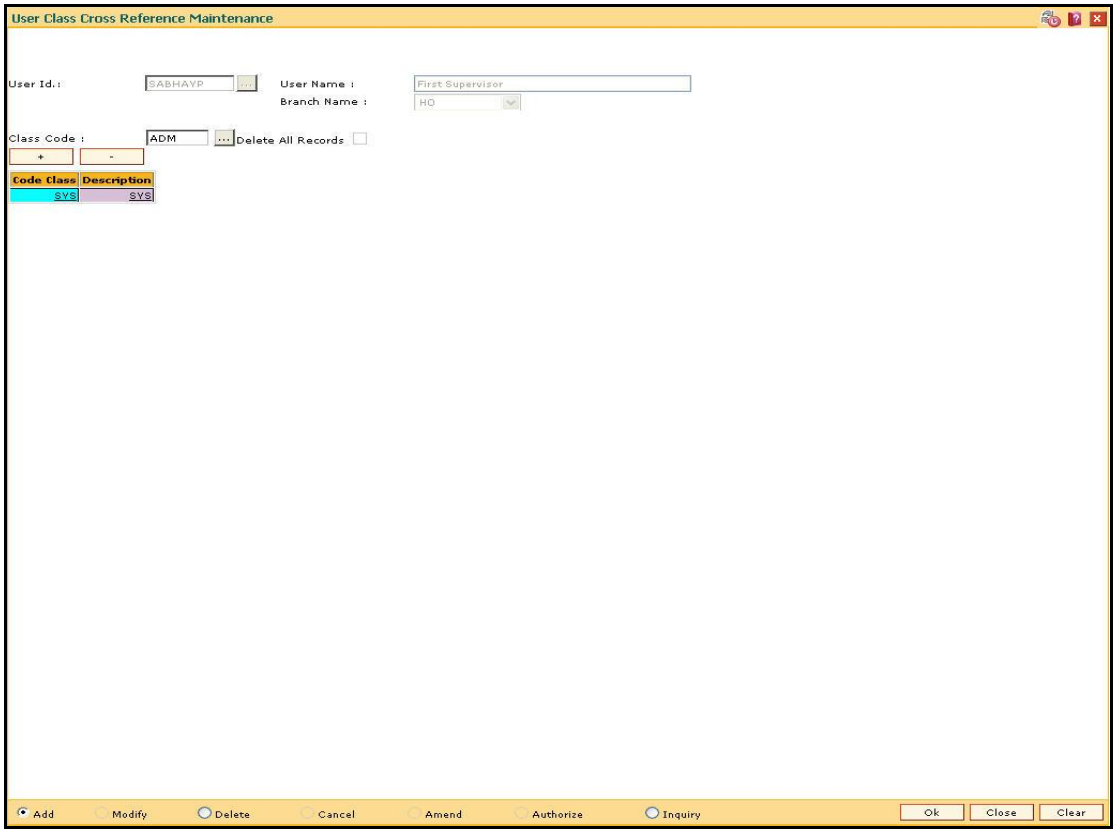
Field Description

Field Name	Description
User Id	[Mandatory, Drop-Down] Select the user ID from the drop-down list. These user ID's are maintained in the **User Profile Maintenance** (Fast Path: SMM02) option.
User Name	[Display] This field displays the user name based on the selected user ID.
Branch Name	[Display] This field displays the branch name to which the selected user ID belongs.
Class Code	[Mandatory, Pick List] Select the class code, for linking the class to a user ID, from the pick list. A valid user should have a class code associated to the user ID. The user can link a user to more than one class.
Delete All Records	[Conditional, Check Box] Select the **Delete All Records** check box to delete the records associated with the user ID. This field is enabled if the user selects the **Delete** mode. This field is non-editable in the **Add** mode.

Column Name	Description
Code Class	[Display] This column displays the class code.
Description	[Display] This column displays the description of the class code.

3. Click the **Add** button.
4. Select the user ID from the drop-down list and select the class code from the pick list.

User Class Cross Reference Maintenance



5. Click the **+** button.
6. The system displays the message "Class code appended to the List". Click the **OK** button.
7. The system refreshes the **User Class Cross Reference Maintenance** screen with the updated fields. Click the **Ok** button.
8. The system displays the "Authorization Required. Do You Want to continue?". Click the **OK** button.
9. The system displays the **Authorization Reason** screen.
10. Enter the relevant information and click the **Grant** button.
11. The system displays the message "Record Added". Click the **OK** button.
12. The user cross reference is added successfully.

1.21. SMM13 - Template Transaction Limits

Using this option limits on financial transactions can be maintained in the system for all users of the system. The limits can be maintained for a group of users under a particular template and currency combination. The online and offline limits for same branch and for inter branch are maintained in this option. You can also populate the limits that are assigned to the transaction group to the individual transaction mnemonics.

Definition Prerequisites

- BAM25 - Currency Definition
- BAM15 - Transaction Mnemonic Codes

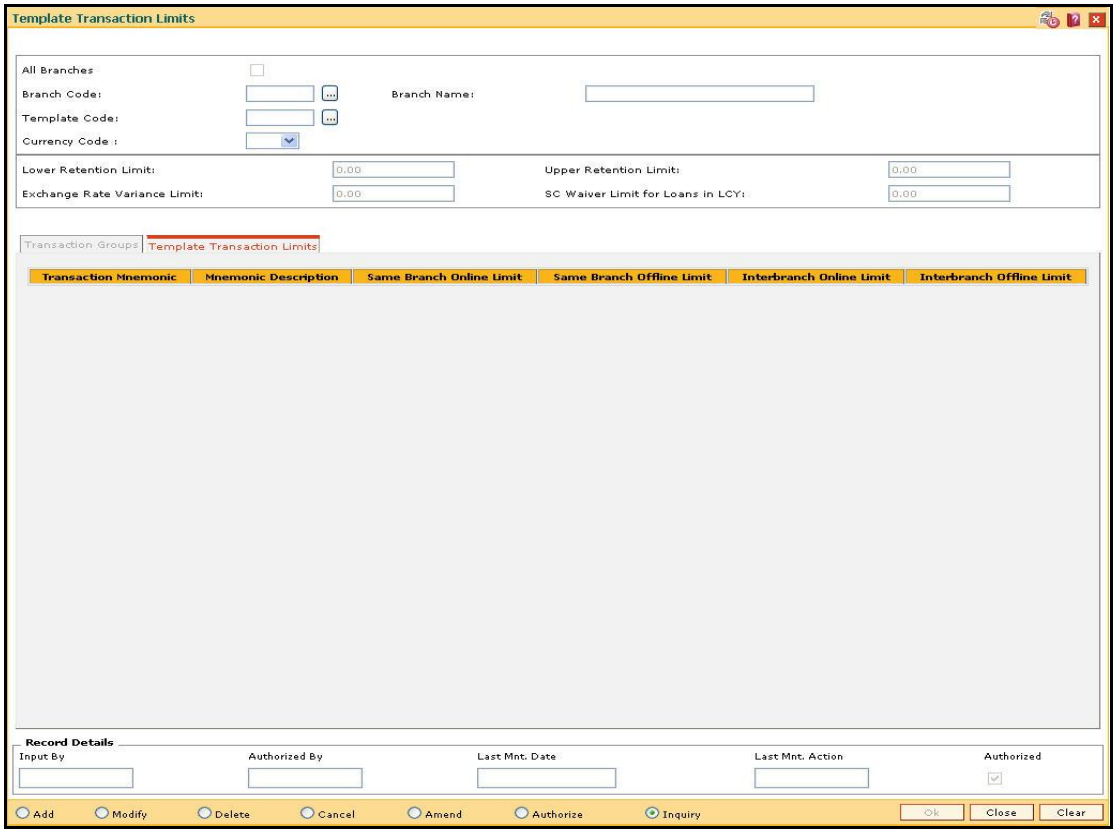
Modes Available

Add, Modify, Delete, Cancel, Amend, Authorize, Inquiry. For more information on the procedures of every mode, refer to Standard Maintenance Procedures.

To add template limits

1. Type the fast path **SMM13** and click **Go** or navigate through the menus to **Global Definitions > Security > Template Transaction Limits**.
2. The system displays the **Template Transaction Limits** screen.

Template Transaction Limits

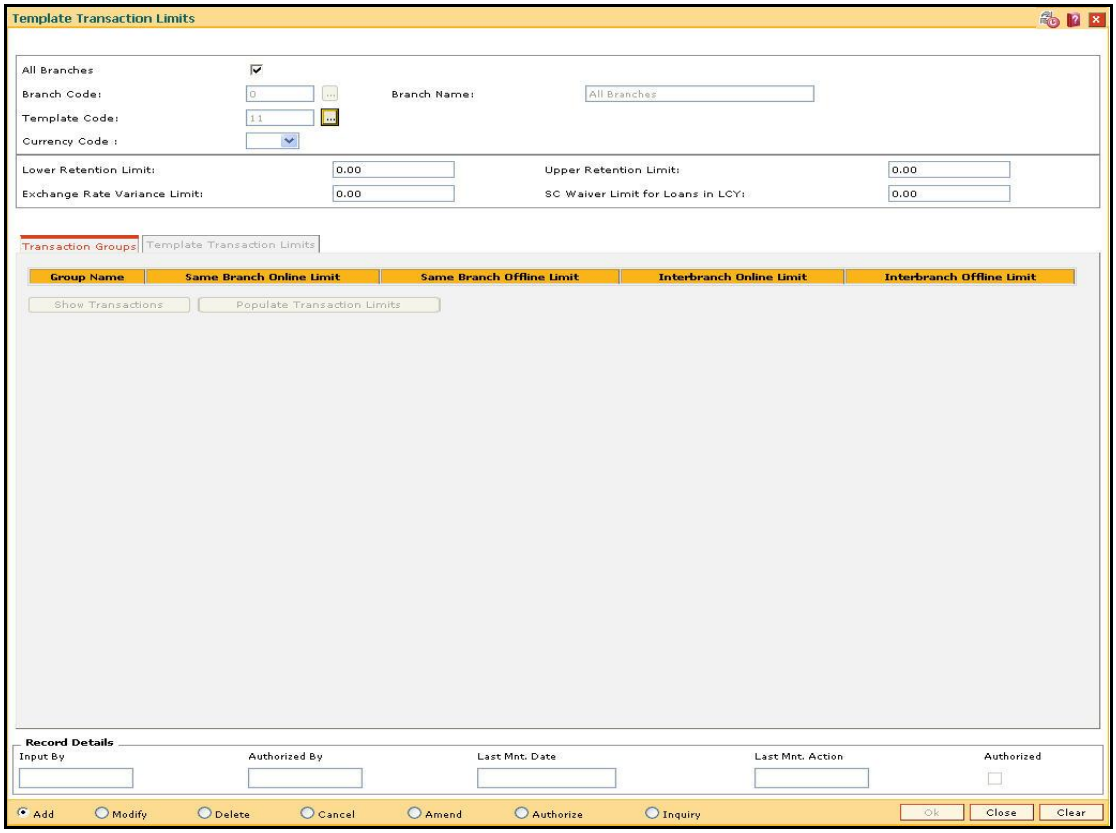


Field Description

Field Name	Description
All Branches	[Optional, Check Box] Select the **All Branches** check box to link the template to all the branches of the bank.
Branch Code	[Mandatory, Pick List] Select the branch code, for which the template is to be defined, from the pick list. By default, it displays the branch code as zero if the **All Branches** check box is selected.
Branch Name	[Display] This field displays the name of branch.
Template Code	[Mandatory, Pick List] Select the template code, for which the limit is to be defined, from the pick list.
Currency Code	[Mandatory, Drop-Down] Select the currency for the template. from the drop-down list The system fetches the data from bank currency maintenance. The drop-down lists all the currencies that are defined in the **Currency Definition** (Fast Path: BAM25) option.
Lower Retention Limit	[Mandatory, Numeric, 10, Two] Type the appropriate lower retention limit for a teller. This is the minimum amount that a teller can retain with himself at the end of the day.
Upper Retention Limit	[Mandatory, Numeric, 10, Two] Type the upper retention limit for a teller. This is the maximum amount that a teller can retain with himself at the end of the day.
Exchange Rate Variance Limit	[Mandatory, Numeric, 10, Two] Type the variance in percentage over base exchange rates that the users linked to this template are allowed to permit.
SC Waiver Limit for Loans in LCY	[Mandatory, Numeric, 10] Type the SC waiver limit for the loan account.

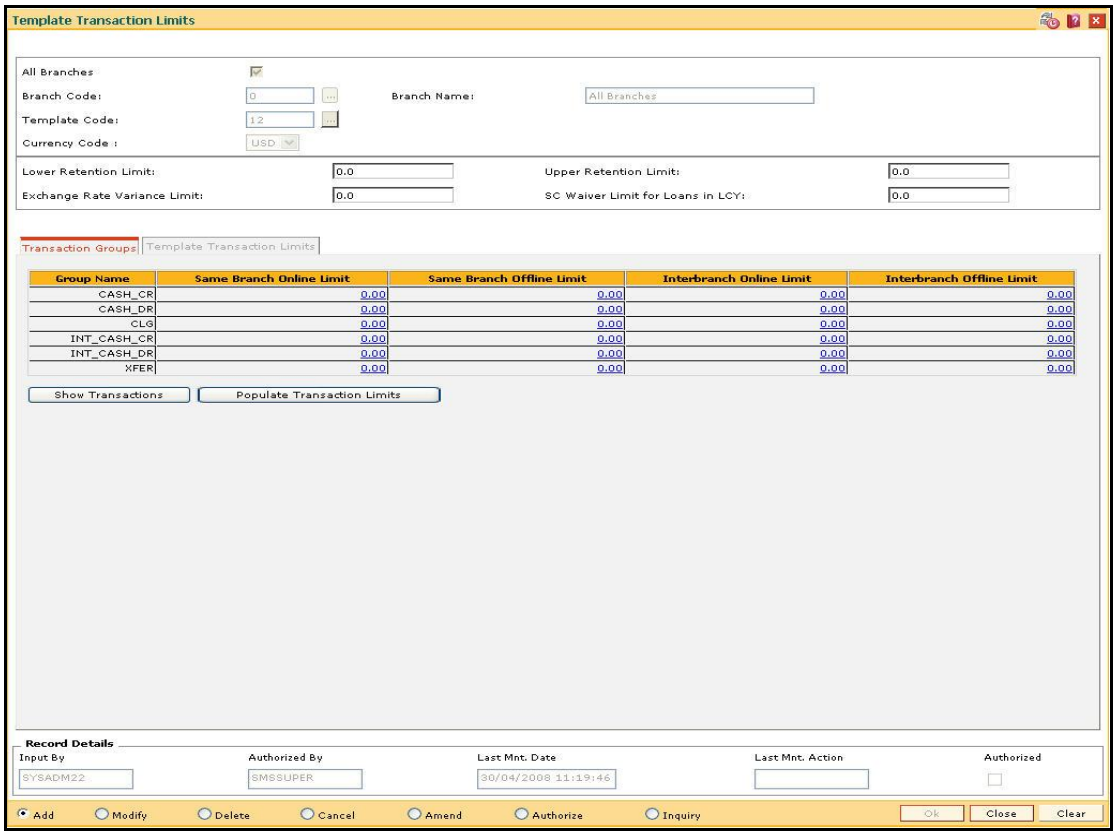
3. Click the **Add** button.
4. Select the **All Branches** check box to link the template to all the branches of the bank.
5. Enter the required information in the various fields.

Template Transaction Limits



6. Enter the required information in the various tab screens.

Transaction Groups

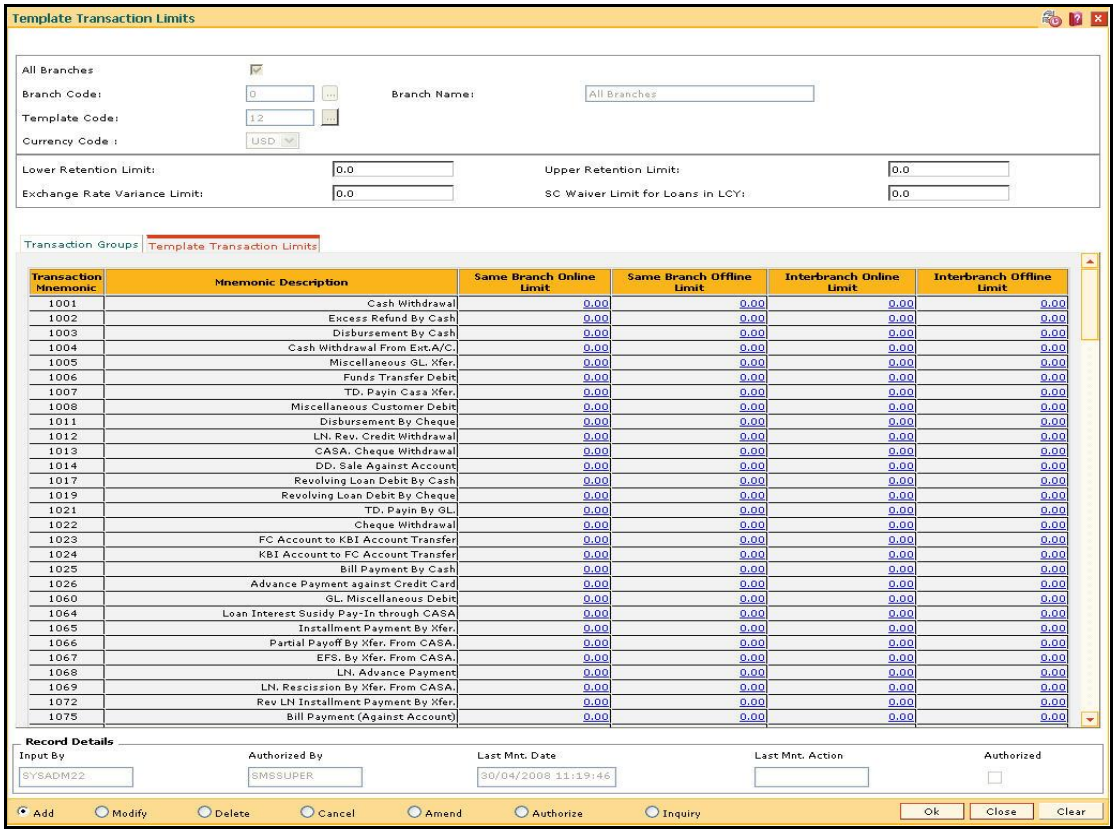


Field Description

Column Name	Description
Group Name	[Display] This column displays the transactions group name. The options are: • CASH_CR: This group lists all the cash debit transaction mnemonics • CASH_DR: This group lists all the cash credit transaction mnemonics • CLG: This group lists all the clearing related transaction mnemonics • INT_CASH_CR: This group lists all the interest cash credit transaction mnemonics • INT_CASH_DR: This group lists all the interest cash debit transaction mnemonics • XFER: This group lists all the transfer related transaction mnemonics

Column Name	Description
Same Branch Online Limit	[Mandatory, Numeric, 10, Two] Type the online transaction limit for the same branch for the corresponding group.
Same Branch Offline Limit	[Mandatory, Numeric, 10, Two] Type the offline transaction limit for the same branch for the corresponding group.
Interbranch Online Limit	[Mandatory, Numeric, 10, Two] Type the online interbranch transaction limit for the corresponding group.
Interbranch Offline Limit	[Mandatory, Numeric, 10, Two] Type the offline interbranch transaction limit for the corresponding group.
Show Transactions	[Command Button] Click the button to view the transactions listed in the selected transaction group. This is only for information purposes.
Populate Transaction Limits	[Command Button] Click the button to populate the limits that are assigned to the transaction group to the individual transaction mnemonics. The system displays the **Template Transaction Limits** screen. The user cannot change the limit assigned to a group once he clicks the **Populate Transaction Limits** button.

Template Transaction Limits



Field Description

Column Name	Description
Transaction Mnemonic	[Display] This column displays the mnemonics of the transactions listed in the transaction group.
Mnemonic Description	[Display] This column displays the description of the transaction mnemonic.
Same Branch Online Limit	[Mandatory, Numeric, 10, Two] Type the online transaction limit for the same branch for the corresponding mnemonic. By default, the system displays the limit specified for the transaction group.

Column Name	Description
Same Branch Offline Limit	[Mandatory, Numeric, 10, Two] Type the offline transaction limit for the same branch for the corresponding mnemonic. By default, the system displays the limit specified for the transaction group.
Interbranch Online Limit	[Mandatory, Numeric, 10, Two] Type the online interbranch transaction limit for the corresponding mnemonic. By default, the system displays the limit specified for the transaction group.
Interbranch Offline Limit	[Mandatory, Numeric, 10, Two] Type the offline interbranch transaction limit for the corresponding mnemonic. By default, the system displays the limit specified for the transaction group.

7. Click the **Ok** button.
8. The system displays the message "Record Added...Authorization Pending". Click the **Ok** button.
9. The template transaction limits are added once the record is authorised.

Security Management System User Manual

May 2013

Version : 5.0.0.0.0

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

www.oracle.com/ financial_services/

Copyright © 2013 Oracle and/or its affiliates. All rights reserved.

No part of this work may be reproduced, stored in a retrieval system, adopted or transmitted in any form or by any means, electronic, mechanical, photographic, graphic, optic recording or otherwise, translated in any language or computer language, without the prior written permission of Oracle Financial Services Software Limited.

Due care has been taken to make this document and accompanying software package as accurate as possible. However, Oracle Financial Services Software Limited makes no representation or warranties with respect to the contents hereof and shall not be responsible for any loss or damage caused to the user by the direct or indirect use of this document and the accompanying Software System. Furthermore, Oracle Financial Services Software Limited reserves the right to alter, modify or otherwise change in any manner the content hereof, without obligation of Oracle Financial Services Software Limited to notify any person of such revision or changes.

All company and product names are trademarks of the respective companies with which they are associated.